

# internal organs

a political hacking scandal	4
the hacker reading list	8
central office operations	12
more leaked documents	16
anatomy of a rip-off	22
letters	24
winning reader entry	32
the word in the street	36
2600 marketplace	41
listings	42

2600 Magazine  
PO Box 752

Middle Island, NY 11953 U.S.A.

Forwarding and Address Correction Requested

SECOND CLASS POSTAGE  
PERMIT PAID AT  
EAST SAGAROCK, N.Y.  
11703  
ISSN 0748-0385

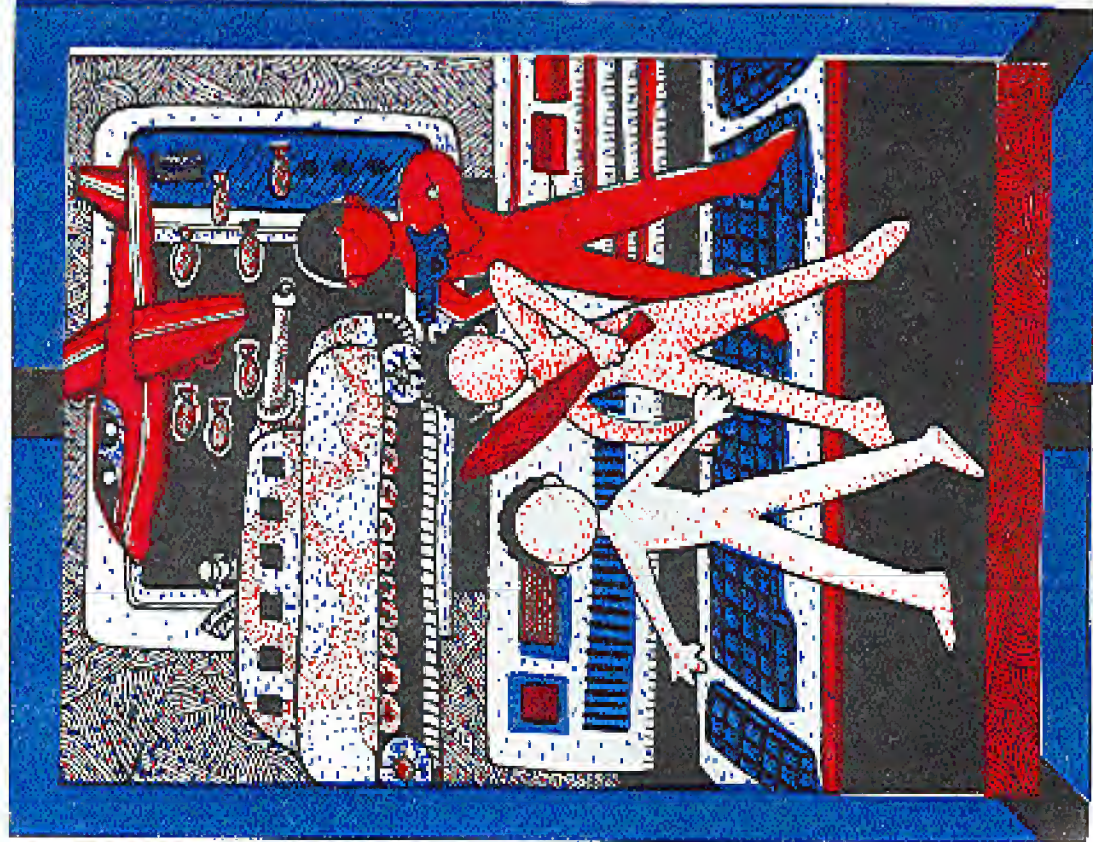
26  
26

# 2600

The Hacker Quarterly

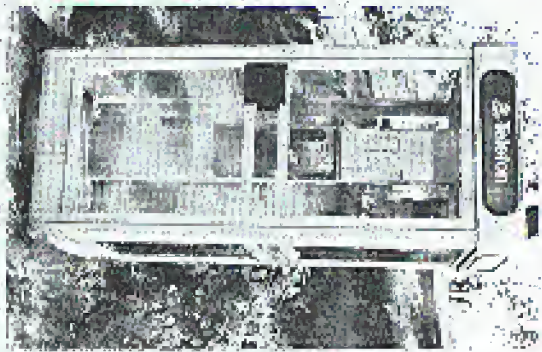
VOLUME SEVEN, NUMBER FOUR

WINTER, 1990

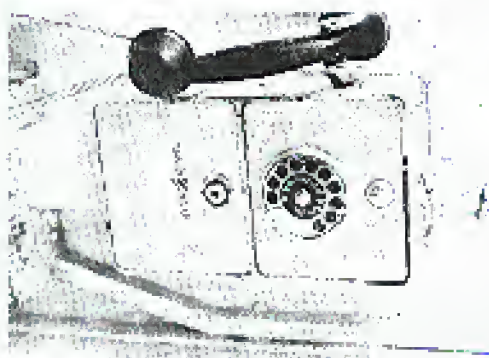
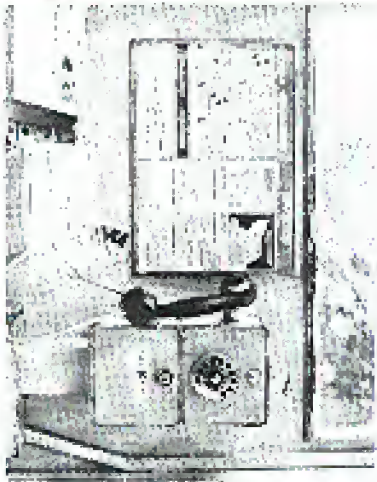




## SCANDINAVIAN PAYPHONES



A SWEDISH PAYPHONE AT DJURGARDSBERG, STOCKHOLM



FINNISH PAYPHONE ON THE ISLAND FORIKRESS OJ  
SUOMENLINNA (SVEABORG), HELSINKI

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99,  
MIDDLE ISLAND, NY 11953. SPECIAL PRIZE FOR AFRICAN PAYPHONES.

2600 (ISSN 0729-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.  
POSTMASTER: Send address changes to  
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (C) 1990, 1991 2600 Enterprises, Inc.  
Yearly subscription: U.S. and Canada --\$18 individual, \$45 corporate (U.S. funds),  
Overseas -- \$30 individual, \$65 corporate.  
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989  
at \$25 per year, \$40 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:  
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.  
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:  
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.  
NETWORK ADDRESS: 2600@world.ica.us

2600 Office Line: 516-751-2600, 2600 FAX Line: 516-751-2608

## STAFF

### Editor-In-Chief

Emmanuel Goldstein / Alan Smithie

### Artwork

Holly Kaufman Spruch

**Writers:** Eric Corley, John Drake, Paul Estey, Mr. French, The Gilch, The Infidel, Log Lady, Craig Neidorf, The Plague, The Q, David Ruderman, Bernie S., Lou Shannon, Silent Switchman, Mr. Upsetter, Violence, Dr. Williams, and the anonymous many.

**Remote Observations:** Geo. C. Tlyou

**Shout Outs:** The subterranean d'esper: Find the Power, dd: your Day will come, we promise; SS: the rules for making it interesting; Franklin: the few who have the strength to face the many; Scaring Target and the future: the million held hostage.



# a political

According to the Philadelphia *Inquirer*, a Republican staff member gained access to as many as 1,000 computer files and documents belonging to Democrats. The GOP staffer, Jeffrey Land, is reported to have admitted tapping into their files "many, many times" between July 1988 and the spring of 1990. Land was apparently able to gain access to files detailing "campaign contributions and the 1991 campaign strategy of the New Jersey Senate Democrats."

What's particularly appalling is that a secret legislative report indicates that his activities were known by his superiors who saw nothing wrong with what he was doing. "No one thought it appropriate to bring this fact to anyone's attention or deemed this to constitute an ethical breach," the report said.

A letter recently received by 2600 claims to reveal some inside information on this case. We'll let you be the judges.

I'd rather not divulge my real name, nor can I divulge my employers' names, not in light of an ongoing criminal investigation. Suffice it to say that I work for one of the two major political parties within the State of New Jersey and that, for the time being, I wish to maintain this job for a little while longer.

I report to the party leadership. I have been involved in politics for quite some time and now do a wide range of duties, among them issues of telecommunications security. My telecommunications security

skills, though hardly noteworthy in the presence of 2600's readership, are somewhat respectable and tremendously aided by publications such as yours. This is why I wish to return a favor and contribute some of my insight for everybody's benefit.

Up front, I have been privy to much of what is going on in regards to the Jeffrey Land case.

Mr. Land was a former Assembly aide to an Assemblyman, an assemblyman who, coincidentally, was among those implicated in the Pete

## "The Legislative

**Network is one system divided into sub-systems. It isn't too hard to get into one sub-system and out the other."**

Those scandal (this assemblyman wrote a letter of recommendation on behalf of the guy who was indicted for participating in a cocaine ring selling to Rose).

Land was smart. We were considered to be among the "bright boys".

Back in '88, we inadvertently broke through the web system of the WANG Legislative Network Systems and had found ourselves within the Systems Administrators' controls.

# hacking scandal

I didn't stick around for too long. The only information I gained was a better understanding of how the system worked, but not the contents of the individual files stored within.

Land also busted through the users' system but didn't back out. He kept going on his own, all through '88, '89, and up to February of 1990 when he finally got caught.

The Land case is fascinating. It's given in the news around here for some time. Land had not only gotten into the system, but had also taken out interesting information, like contributor listings, campaign strategies, and such — all from the opposing political party.

The Legislative Network, you see, is one system divided into sub-systems. It isn't too hard to get into one sub-system and out the other. This is essentially what Land did.

Inquiries by the State Ethics Committee determined that the party leadership whom Land was working for was not only aware of this, but "saw nothing wrong in what he was doing."

Incredible. What's even more fascinating is that the opposing political party whose files have been exposed are not seeking to press any charges and wish to instead "forget about the whole thing." This, despite the acknowledged fact that Land managed to see and/or obtained well over 1,000 individually protected files!

Why back down?  
Here's why:  
Land uncovered solid, hard evidence including:

- 1) State staff, hired solely for the benefit of service to the public were

working solely for the benefit of the elected officials on public money and time using public facilities, notably computer databasing facilities and the like. Public tax money for state staff salaries was therefore used to keep elected officials in office. Everybody does this, but it's not supposed to be known outside of the office.

2) Land's computer evidence directly correlates between given contributions and posted legislation. The major stumbling block for election-law overseers is that you cannot readily tell who is being given what. PAC (Political Action Committee) money is handed out in such a way that election law reports do not readily tell who actually benefits from these contributions. PAC's are deliberate fronts for corporations and others who do not want to leave a trail. Land obtained evidence showing what

**"How can we reasonably expect our legislators to legislate on our behalf on such crucial telecommunications matters when they are, in fact, among those breaking the law?"**

corporation gained what piece of legislation — tax breaks, funding loopholes, etc. — in a manner never done before.

**More Weirdness**  
Election-law controls are obviously



# a hacking

in need of expansion. In light of what happened in the fall of '89, the Land case underlines this point. During October of '89, the current majority leadership members were implicated in a so-called "shake-down" of a lawyer's PAC. Among the so-called statements said to the lawyer's PAC representatives during that fateful dinner meeting was the now famous line: "Your members are going to be upset if your bills don't get posted." The FBI and the Attorney General's office later exonerated them of the allegations, but a bad taste still lingers. We've all known about this shit:

**"It's not how you play the game, it's whether you win. Winning is, after all, everything."**

corruption is as old as the human race. A politician taking money — so what else is new? The catch is how can we reasonably expect our legislators to legislate on our behalf on such crucial telecommunications matters when they are, in fact, among those breaking the law? Our legislators are among those encouraging partisan hacking!

I recall vividly what our director for our legislative staff said to me: "It's not how you play the game, it's whether you win. Winning is, after all, everything."

Great. It is utterly ironic that, when approached upon the issue of "hackers" and the like, legislators crank out their total distaste toward these individuals" while all along whatever information hackers culled they greedily accept, seeing "no apparent ethical wrongdoing" as Land's superiors so stated.

The State Attorney General's office announced that they "see no need to further investigate the matter." The Speaker of the House said that "the public doesn't give a tinker's damn about the situation." The argument flowing to the newspapers about the "fundamental separation of powers between the legislative and the executive branch of government" is garbage. The separation argument is, actually, a means of cuckooing the real issue: election funding reform. Ironically, both partisan political parties, Republican and Democrat, do agree upon avoiding this one issue as next year's elections are looming on the horizon.

I write this because you state in your article on "Operation Sundevil" that we should write to our legislators. Actually, as one who works closely with legislators, they really don't "give a tinker's damn", unless, of course, you're a large, multi-national PAC. After helping to set up the fundraisers, I've watched the legislative bills get posted and know there's no such thing as coincidence at the state capital.

I, for my part, feel that this country is rapidly becoming a tremendously twisted nightmare; it's one thing to have soldiers goosestepping down

# political scandal

Pennsylvania Avenue, but something else when we're living within a giant David Lynch sitcom.

It is time that we start politicizing ourselves. (Has a hacker's PAC, anyone?) It's time to start working together before more shit comes down the pike. Expect to see regulations, BBS licensing, and the like to come about, all in the name of raising taxes for these "tough economic times". Taxation and operational regulations are what the Secret Service and the legislators want, both as a means of a "better regulatory/enforcement" and for raising more money to channel into other programs or job perks for

**"The computer expert is becoming the samurai of these petty lords."**

revenues on tea payoffs.

Never mind, though, that most of the boards would go under due to lack of sufficient funds to keep them going. This scenario also doesn't mention that those remaining BBS's would do so only by charging or increasing their operational charges. Our cutting edge gets dull and us with it — unless, of course, you've become a member of The New Movement, the Underground Net.

**It's Getting Cold Around Here**

Several other trends are becoming evident: the winnowing of Freedom of Information Act file acquisitions (see June of '90 American Bar Association

Magazine), the lack of accountability on the part of credit bureaus obtaining private information from branches of the U.S. government (isn't it an amazing coincidence that TRW, the credit bureau, is also TRW, the major defense industry corporation?), and now the crackdown on BBS's — yep, surf's up; the storm's rising, gang.

**The Lords of Disorder**

Watergate lives on. I was recently hired by a congressman on their campaign "telecommunications-database system. Somebody broke into the congressman's system and got a listing of the major databases. No disks were stolen or damaged, not that anything ever is, and the office doors were, interestingly enough, not forced open. After an "inter-office investigation", custodial staff was found to have been "lax" and, although not proven, it appears that it was a primary election candidate's woker who managed to get in and check out the files.

This was bad. Once you know when, where, who, and what voting block your opponent is gunning, well, then you're tucked. Political strategy must then be shifted accordingly, and this can be a real pain in the ass.

This last story and the Land case illustrates how the computer expert is becoming the samurai of these petty lords, particularly those experts who stand on "the edge". Perhaps herein lies our true strength.

We are far stronger than what we're given to be; this is why the SIS is strong-arming us and why corrupt politicians employ our skills while yet taking our life's blood.











# Central Office

This is one of the last articles to come out of *The Legion of Doom* by Agent Steel

I should point out that the information in this article is correct to the best of my knowledge. I'm sure there are going to be people that disagree with me on some of it particularly the references to tracing. However, I have been involved in telecommunications and computers for 12 years.

I'm basing this article around the 1AESS since it is the most common switch in use.

## Outside Plant

This is the wiring between your telephone and the central office. That is another article in itself so if you are interested read Phucked Agent D's article in an outside loop in the LOD Technical Journal. It explains those green boxes you see on street corners, aerial cables, manholes, etc. Where it stops, this article stops.

## Cable Vault

All of the cables from other offices and from subscribers enter the central office underground. They enter into a room called the cable vault. This is a room generally in the basement located at one end or another of the building. The width of the room varies but runs the entire length of the building. Outside cables appear through holes in the wall. The cables then run up through holes in the ceiling to the frame room.

Understand that these cables consist of an average of 3500 pairs of wires. That's 3500 telephone lines. The amount of cables obviously depends on the size of the office. All cables — interoffice, local lines, fiber optic, coaxial — enter through the cable vault.

## Frame Room

The frame is where the cable separates to individual pairs and attaches to connections. The frame runs the length of the building from floor to ceiling. There are

two sides to the frame, the horizontal side and the vertical side. The vertical side is where the outside wiring attaches and the protector fuses reside. The horizontal side is where the connectors to the switching system reside. Multi-conductor cables run from the connectors to actual switching equipment. So what we have is a large frame called the Main Distribution Frame (MDF) running the entire length of the building, floor to ceiling 5 feet thick. The MDF consists of two sides, the VDF and the HDF. Cables from outside connect on one side and cables from the switching equipment connect to the other. Juniper wires connect the two. This way any piece of equipment can be connected to any incoming "cable pair". These juniper wires are simply 2 conductor twisted pair running between the VDF and HDF.

What does all this mean? Well, if you had access to COSMOS you would see information regarding cable end pair and "OE" or originating equipment. With this you could find your line on the frame and on the switch. The VDF side is clearly marked by cable and pair at the top of the frame, however the HDF side is a little more complicated and varies in format from frame to frame and from one switch to another. Since I am writing this article around the 1AESS, I will describe the OE format used for that switch.

OE ASB-ODD-EFF where: A = Control group (when more than one switch exists in that C.O.); B = LN Line Link Network; C = LS Line Switching Frame; D = CONC or concentrator; E = Switch (individual, not the big one); F = Level. There is one more frame designation called LOC or location. This gives the location of the connector block on the HDF side.

Switching Systems  
Writing an article that covers them all would be lengthy indeed. So I am only going to list the major ones and a brief description of each.  
Step by Step (Strowger 1893). First automatic, required no operators for local

# Operations

calls, no custom calling or touch tone, manufactured by many different companies in different versions, hard wire routing instructions, could not choose an alternate route if programmed route was busy. Even dial pulse ripped a "stepper" type relay to find its path.

No. 1 Crossbar (1930) - No. 5 Crossbar (1947) (later, more capacity). Western Electric, first ability to find idle trunks for call routing, no custom calling or equal access, utilized a 10x20 cross point relay structure, hard wired common control logic for program control, also copied by other manufacturers.

No. 4 Crossbar. Used as a toll switch for AT&T's long line network. 4-wire tandem switching, not usually used for local loop switching.

No. 1ESS (1968) - No. 1AESS (1973). Western Electric, described in detail later in this issue.

No. 1EAX. GTE Automatic Electric, GTE's version of the 1AESS, slower and louder.

No. 2ESS (1967) - No. 2AESS (1974). Western Electric, analog switching under digital control, very similar to the No. 1ESS and No. 1AESS, downsized for smaller applications.

No. 3ESS. Western Electric, analog switching under digital control, even smaller version of No. 1AESS, rural applications up to 4500 lines.

No. 2EAX. GTE Automatic Electric, smaller version of 1EAX, analog switch under digital control.

No. 4ESS. Western Electric, toll switch, 4-wire tandem, digital switching, uses the 1AESS processor.

No. 5EAX. GTE, is there a patron here? No. GTE Digital toll switch, 4-wire tandem switching.

No. 8ESS. AT&T Network Systems, full scale computerized digital switching, ISDN compatibility, utilizes time sharing technology, toll or end office.

GMS 100 Digital Master Switch. Northern Telecom, similar to 5ESS, runs

power, considerably less expensive.  
GMS 200. Toll and Access Tendon, optional operator services.

GMS 250. Toll switch designed for common carriers.

GMS 300. Toll switch for international gateways.

No. 5EAX. GTE Automatic Electric, same as 5ESS.

How much does a switch cost? A fully equipped 5ESS for a 40,000 subscriber end office can cost well over 3 million dollars. Now you know why your phone bill is so much. Well, maybe your parents bill.

## The 1ESS and 1AESS

This was the first switch of its type placed into widespread use by Bell. Primarily an analog switch under digital control, the switch is no longer being manufactured. The 1ESS has been replaced by the 1EAX and other full scale digital switches. However, it is still by far the most common switch used in today's class 5 end offices.

The #1 and #2 use a crosspoint switching matrix similar to the crossbar. The primary switch used in the matrix is the 1EAX (hereinafter in the 1A, it is a two-state or signed a-10 switch. It is basically a magnetic switch that does not require voltage to stay in its present position. Voltage is only required to change the state of the switch.

The #1 utilized a computer style control system and memory. Memory used by the #1 changed with technology, but most have been upgraded to RAM. Line scanners monitor the status of customer lines, crosspoint switches, and all internal output; and incoming trunks, separating their status to the central control. The central control then either calls upon program or call store memories to cross which elements to activate for processing the call. The crosspoint matrices are controlled via central pulse distributors when in turn are controlled by the central control via data buses. All of the scanners, AYA tape controllers, pulse distributors, x-



## What Makes A

point matrix, etc., listen to data buses for their address and command or report their information on the buses. The buses are merely cables connecting the different units to the central control.

The IE was quickly replaced by the IA due to advances in technology. So IAs are more common. Also, many of the IEs have been upgraded to IAs. This meant changing the board to the renewed relay, adding additional peripheral component controllers (ie free up central controller loads) and implementation of the IA processor. The IA processor replaced older style electronics with integrated circuits. Both switches operate similarly. The primary differences were speed and capacity. The #1ESS could process 110,000 calls per hour and serve 120,000,000 lines.

Most of the major common control elements are either fully or partially duplicated to ensure reliability. Systems run simultaneously and are checked against each other for errors. When a problem occurs, the system will doublecheck, reroute, or switch over to auxiliary to continue system operation. Alarms are also reported to the maintenance console and are in turn printed out on a printer near the control console.

Operation of the switch is done through the Master Control Center (MCC) panel and/or a terminal. Remote operation is also done through input/output channels. These channels have different functions and therefore receive different types of output messages and have different abilities as far as what type of commands they are allowed to issue. Here is a list of the commonly used TTY channels.

- Maintenance:** Primary channels for testing, enable, disable, etc.
- Recent Change:** Changes in class of service, calling features, etc.
- Administrative:** Traffic information and control.
- Supplementary:** Traffic information supplied to automatic network control.

**SCC Maint:** Switching control centers interface.

**Plant Service Center:** Reports testing information to test facilities.

At the end of this article you will find a list of the most frequently seen Maintenance channel output messages and a brief description of their meanings. You will also find a list of frequently used input messages.

There are other channels as well as backups but the only ones to be concerned with are Recent Change and SCC Maint. These are the two channels you will most likely want to get access to. The Maintenance channel doesn't leave the C.O. and is used by switch engineers as the primary way of controlling the switch. During off hours and weekends the control of the switch is transferred to the SCC.

The SCC is a centrally located bureau that has up to 25 switches reporting to it via their SCC maint channel. The SCC has a multi-processor running SCCS that watches the output of all these switches for trouble conditions that require immediate attention. The SCC personnel then has the ability to input messages to that particular switch to try and correct the problem. If necessary, someone will be dispatched to the C.O. to correct the problem. I should also mention that the SCC maint has dialups and access to SCCS means access to all of the switches connected to it.

The Recent Change channels also connect to a centrally located bureau referred to as ROMAC. These bureaus are responsible for activating lines, changing class of service, etc. ROMAC has been automated to a large degree by computer systems that log into COSMOS and look for pending orders. COSMOS is basically an order placement and record keeping system for central office equipment, but you should know that already, right? So this system called MIZAR logs into COSMOS, pulls orders requiring recent change work, then in one batch several times a day, transmits the orders to the appropriate

## Central Office Tick

switch via its Recent Change Channel

Testing of the switch is done by many different methods. Bell Labs has developed a number of systems, many accomplishing the same functions. I will only attempt to cover the ones I know fairly well.

The primary testing system consists of the trunk test panels located at the switch itself. There are three and they all pretty much do the same thing: test trunk and line paths through the switch.

**Trunk and Line Test Panel**  
**Supplementary Trunk Test Panel**  
**Manual Trunk Test Panel**

MLT Mechanized Loop Testing is another popular one. This system, often available through the LMOS database, can give very specific measurements of line levels and losses. The "Ty Mask" is also popular giving the user the ability to monitor lines via a call back number.

**DAMT Direct Access Mechanized**  
Testing is used by line repairman to put you on numbers to help them find lines. This was previously done by Frame personnel, so this automates that task. DAMT can also monitor lines, however the audio is scrambled in a manner that slows one only to tell what type of signal is present on the line, or whether it is busy or not.

All of these testing systems have one thing in common. They access the line through a No Test Trunk. This is a relay (in the 1ESS) which can drop in on a specific path or line and connect it to the testing device. The test trunks are part of the switch itself and act like a telephone line into the switch. The function of this line is strictly for access and testing of subscriber lines. It depends on the device connected to the trunk, but there is usually a noticeable click heard on the tested line when the No Test Trunk drops in. Also the testing devices I have mentioned here will seize the line, busying it out. This will present problems when trying to monitor calls — you would need to drop in on calls in progress. The No Test Trunk is also the

method in which operator consoles do redactions and interrupts.

**Intelligence Signaling**

Calls coming into and leaving the switch are routed via trunks. The switches select which trunk will route the call most effectively and then reserve the dialled number to the distant switch. There are several different ways this is done. The two most common are Loop Signaling and CCIS. Common Channel Intelligence Signaling. The predecessor to both of these is the farbus and almost extinct 9F Signaling. This utilized the presence of 2600 Hz to indicate trunk in use. If one wishes 2600 Hz down one of these buses, the distant switch would think you hung up. Remove the 2600, and you have control of the trunk and you could then MF your own number. This worked great for years. Assuming you had dialed a toll-free number to begin with, there was no billing generated at all. The 1AESS does have a program called SIGI that looks for any 2600, works after the original connection of a call call it then proceeds to record on ANM and output any MF digits received. However due to many long distant carriers using signaling that can generate these messages it is often overlooked and "SIGI RR" output messages are quite common.

Loop signaling still uses MF to transmit the called number to the distant switch. However, the polarity of the voltage on the trunk is reversed to indicate trunk use. CCIS, sometimes referred to as COSAS, uses a separate data link sending packets of data consisting information regarding outgoing calls. The distant switch monitors the information and connects the connect trunk to the central path. This is a faster and more efficient way of call processing and is being implemented all over. The process that AT&T uses is COS7 and is currently being accepted as the industry standard. COS6 and COS7 are somewhat similar.

Intelligence trunks are multiplexed together onto one pair. The standard is 24



# leaked

ATTACHED 1

CLASSIFICATION

Definitions and Examples of Discourteous Actions Which Violate Current Discipline:

## 1. NOT RESPONSIVE:

**Definition:** Not exhibiting love and respect felt to be appropriate in business - e.g., talking in a joking or laughing manner at inappropriate times, use of slang - non-standard vocabulary.

**Example:** Customer: "I would love to call person to person the Sales Manager."

**Operator:** "Get ya." "Does he have a name and given the number."

"Oh, calling a pig what today?"

## 2. NOT ANIMATED/NO ANSWER:

**Definition:** Refusal to accept or action ill-mannered, abrupt, curtly, unresponsive, egotistic, arrogant, unwilling to provide assistance, terse responses.

**Example:** Customer: "Operator, did you say the area code was 710 or 213?"

**Operator:** "Yes, because with you in you don't listen." "I'll call you once more 2-1-1 and don't ask again."

"Could you understand English?" "I said 2-1-1!"

**Example:** Customer: "When are I going to get my number, Operator?"

**Operator:** "Doesn't I had any my identification?" "If you weren't so dumb you could call 211 to yourself."

"Does I call like that?" "Does't rush me!"

# documents

## 1. SPEAKING TONE:

### A. Exalted:

**Definition:** To behave by strong, overdone or vulgar statements, impudent.

**Example:** "Hey, operator what time you been out of office?" "I'm ready fast together call."

**Definition:** "What are you doing?" "How the hell do you think you are, someone responsible?" "I've pay let's know of your O.D. Operator."

"Customer, did you give me a pain - see how much?"

### B. Dismissive:

**Definition:** Disparaging, repulsive, using foul, nasty, vulgar, unflattering.

**Example:** Customer: "When connected to work a week, number, can try it again."

**Operator:** "Oh, what's your name, like you want to know?"

"Tough, kiss my ass!"

The above examples are intended to be the random description of each category.

THIS COMES FROM AN UNNAMED PHONE COMPANY'S MANUAL FOR SUPERVISORS. DOESN'T IT JUST PROVE YOUR A--?



# Central Office

(continued from page 15)

channels per pair. This is called T-1 in its analog format and D-1 in its digital format. This is often referred to as carrier or CRR. The terms frame error and phase jitter are part of this technology which is often a word in itself. This type of transmission is effective for only a few miles on twisted pair. It is often common to see maintenance repairs in manholes or special huts. Repeaters can also be found within C.O.s, amplifying trunks between offices. This equipment is usually handled by the "center" room, often on another floor. Carrier also handles special circuits, private lines, and foreign exchange circuits.

After a call reaches a Toll Switch, the transmit and receive paths of the calling and called party are separated and transmitted on separate channels. This allows better transmission results and allows more calls to be placed on any given trunk. This is referred to as 4 wire switching. This also explains why during a call one person can hear cross-talk and the other can't. Cross-talk is bleed-over from other channels on the multiplexed T-Carrier transmission lines used between switches.

### Call Tracing

So with local signaling standard format there is no information being transmitted regarding the calling number between switches. This therefore causes the call tracing routine to be at least a two-step method. This is assuming you are trying to trace an activated call, not one in progress. When call trace (CTD) is placed on a number, a message is output every time someone calls that number. The message shows up on most of the ESS output channels and gives information regarding the time and the number of the incoming trunk group. If the call came from within that office, then the calling number is printed in the message. Once the trunk group is known, it can usually be determined what C.O. the calls are coming from. This is also assuming that the calls are coming from within that Bell company and not through a long distance carrier.

(LEC). So if Bell knows what C.O. the calls are coming from, they simply put the called number on the C.I. list of that C.O. Anytime anyone in that C.O. calls the number in question another message is generated showing all the pertinent information.

Now if this were a real time trace, it would only require the assistance of the SOC and a few commands sent to the appropriate switches (i.e. NET-LINE). This would give you the path and trunk group numbers of the call in progress. Naturally, the more things the call is going through, the more people will need to be involved in the trace. There seems to be a common misconception about the ability to trace a call through some of the larger packet networks like Telenet, Well, I can assure you, Telenet can trace a call through their network in seconds and all that is needed is the cooperation of the Bell companies. Call tracing in itself is not that difficult these days. What is difficult is getting the different organizations together to cooperate. You have to be doing something relatively serious to warrant tracing in most cases, however, not always. So if tracing is a concern, I would recommend using as many different companies at one time as you think is necessary, especially US Sprint. They can't even tell people on time much less trace a call.

### Equal Access

The first thing you need to understand is that every LEC (Inter-Exchange Carrier) — or long distance company — needs to have an agreement with every LEC (Local Exchange Carrier) — or your local phone company — that they want to have access to and from. They have to pay the LEC for the type of service they receive and the amount of trunks, and trunk use. The cost is high and the market is a zoo. The LECs have the following options:

**Feature Group A:** This was the first access plan offered to the LECs by the LECs. Basically whenever you access an LEC by dialing a regular 7 digit number (POTS line), this is FGA. The LEC's

# Operations

equipment would answer the line, interpret your digits, and route your call over their own network. That they would pick up an outgoing telephone line in the city you were calling and dial your number locally. Basically a dial in, dial out situation similar to PG pursuit.

**Feature Group B:** FGB is \$50,000. This is a very different setup from FGA. When you dial 955, your local switch routes the call to the closest Access Tandem (Toll Switch) in your area. There the LECs have direct trunks connected between the AT and their equipment. These trunks usually use a form of multiplexing like T-1 carrier with wind start (2500Hz). On the incoming side, calls coming in from the LEC are basically connected the same way. The LEC WFs into the AT and the AT then connects the calls. There are a lot of different ways FGB is technically set up, but this is the most common.

Tracing on 955 calls has been an area of controversy and I would like to clear it up. The answer is yes, it is possible, but like I mentioned earlier, it would take considerable manpower which equals expensive to do this. It also really depends on how the LEC interface is set up. Many LECs have trunks going directly to class 5 end offices. So if you are using a small LEC, and they figure out what C.O. you are calling from, it wouldn't be out of the question to put CUID on the 955 number. This is highly unlikely and I have not heard from reliable sources of it ever being done. Furthermore, CUID generates a message every time a call is placed to that number. Excessive call trace messages can crash a switch. However, I should mention that brute force tracking of 955s is easily done and relatively easy to track if the LEC is really having a problem in a particular area, they will pursue it.

**Feature Group C:** FGC is reserved for and used exclusively by AT&T.

**Feature Group D:** FGD is similar to FGB with the exception that ANI is used to the LEC. The end office switch must have Equal

Access capability in order to transmit the ANI. Anything above a crossbar can have it. I guess I should mention that it is possible for a crossbar to have it with modifications. FGD can only be implemented on 800 numbers and if an LEC wants it, they have to buy the whole prefix. You should also be aware that long distance companies offer a service where they will transmit the ANI to the customer as well. You will find this being used as a security or marketing tool by an increasing amount of companies. A good example would be 800-998-CHAT.

### IAES\$ Common Output Messages

(Messages is followed by a description.)

- A201: Office alarm
  - A202: Alarm retired or transferred
  - AP23: Fuse blown
  - A304: Unknown alarm scan point activated
  - A905: Correlative power failure
  - AP06: Switchroom alarm via alarm grid
  - AB07: Power plant alarm
  - A508: Alarm circuit battery loss
  - AP08: AVA bus fuse blown
  - A910: Alarm configuration has been changed (renewed, inhibited)
  - AH11: Power converter trouble
  - AR13: Carrier group alarm
  - AR15: Hourly report on building and power alarms
- Automatic Trunk Test**
- AT01: Results of trunk test
- Carrier Group**
- CG01: Carrier group in alarm
  - CG03: Reason for alarm
- Coin Phone**
- CH02: List of pay phones with coin disposal problems
  - CH03: Possible trouble
  - CH04: Phone taken out of service because of possible coin fraud
- Copy**
- CC07: Data copies from one address to another
- Call Trace**
- CTD1: Manually requested trace line to line, information follows



# Inner Workings

- CT02: Manually requested trace line to bank, interactor follows
- CT03: Interactor called placed to a number with CLID
- CT04: In-office called placed to a number with CLID
- CT05: Call placed to number on the CLIST
- CT06: Contacts of the CLIST
- CT07: ACD related trace
- CT08: ACD related trace
- CT09: ACD related trace
- Digital Carrier Trunk**
- DC1 COUNTS: Count of T carrier errors
- Memory Diagnostics**
- DGN: Memory failure in ccps diagnostic program
- Digital Carrier "Frame" Errors**
- FM01: DC1 alarm activated or reset
- FM02: Possible failure of entire bank, not just frame
- FM03: Error rate of specified dgroup
- FM04: Digroup out of frame more than indicated
- FM05: Operation or release of the loop terminal relay
- FM06: Result of digroup circuit diagnostics
- FM07: Carrier group alarm status of specific group
- FM08: Carrier group alarm count for dgroup
- FM09: Hourly report of carrier group alarms
- FM10: Fusible switched digital capacity failure
- FM11: PUC count of carrier group errors
- Maintenance**
- MA02: Status requested print out of MA01 search pad
- MA03: Hourly report of system circuits and units in trouble
- MA04: Reports condition of system
- MA05: Maintenance interrupt count for last hour
- MA06: Scanners, network, and signal detectors in trouble
- MA07: Successful switch of duplicated unit (program store etc.)
- MA08: Excessive error rate of named unit
- MA09: Power faults not be removed from named unit
- MA10: OK to remove paper
- MA11: Power manually removed from unit
- MA12: Power restored to unit
- MA13: Indicates central control active
- MA15: Hourly report of number of times interrupt recovery program called
- MA21: Census data link power removed continued
- MA21: Reports action taken on MA0-REX
- MA22: 4 min. report, energy, action phase lingers are inhibited
- Memory**
- MI02: List of circuits in trouble in memory
- Network Trouble**
- NI01: Network frame unable to switch off line after fault detection
- NI02: Network path trouble Trunk to Line
- NI03: Network path trouble Line to Line
- NI04: Network path trouble Trunk to Trunk
- NI05: Hourly report of network frames made busy
- NI10: Network path failed to restore
- Operating System Status**
- OP ABS-2
- OP APSTRATUS
- OP CHAN
- OP DISRPC: Source of critical alarm, automatic every 15 minutes
- OP OSSSTATUS: Call store status
- OP INSTATUS: Data unit status
- OP EMAPDATA: Error analysis database output
- OP INHINT: Hourly report of interrupted devices
- OP LIBSTAT: List of active library programs
- OP OCCSUNITS: Units out of service
- OP SSSTAT US: Program store status
- Plant Measurements**
- PM01: Daily report
- PM02: Monthly report
- PM03: Response to a request for a specific section of report
- PM04: Daily summary of IC-TEC irregularities
- Report**
- REP T-ADS FUNCTION: Reports that an ADS function is about to occur
- HEPT ADS FUNCTION DUPLEX FAILED

# of a Central Office

- No ADS assigned
- REP T-ADS FUNCTION S-MPLEX: Only one tape drive is assigned
- REP T-ADS FUNCTION STATE CHANGE: Change in state of ADS
- REP T-ADS PROCEDURAL ERROR: You fucked up
- REP T-LINE INBL: Too many permanent outlocks, may indicate bad cable
- REP T-PROG COUNT OFF NORMAL: System program's status off or on
- REP T-RC CENSUS: Hourly report on recent changes
- REP T-RC SOURCE: Recent change system status INDS-1 Tests RC Chan inhibited
- Recent Change**
- RC15: RC message response
- Remove**
- RMV: Removed from service
- Restore**
- RST: Restored to service status
- Ringing and Tone Plant**
- R104: Status of ring zone
- Software Audit**
- SAC1: Call store memory audit results
- SAC3: Call store memory audit results
- Signal Irregularity**
- SVG IRR: Blue box detection
- SG IRR-RELB: LED Detector all
- SVG IRR TRAF: Half hour report of traffic data
- Traffic Condition**
- TC15: Reports owner traffic condition
- TC02: Reason test position test was dialed
- TC03: Same as above
- Trunk Network**
- TN01: Trunk aggregate found trouble
- TN02: Clear tone busy alarm failure
- TN04: Trunk ring request for test panel
- TN05: Trunk test procedural report or overals
- TN06: Trunk test change
- TN07: Response to a trunk you and expect request
- TN08: Failed ringing or ringing call
- TN09: Network ring failures
- TN10: Response to TRK-LIST input usually a request for test position
- TN11: Hourly, status of trunk undergoing lease
- TN12: Daily summary of precut trunk groups
- Traffic Overload Condition**
- TO001: Serious traffic condition
- TO002: Reports status of less serious overload conditions
- Translation (shows class of service, calling features, etc.)**
- TR01: Translation information, response to VFN-ON
- TR03: Translation information, response to VFN-LEN
- TR05: Translation information, response to VFN-NSVY
- TR02: Dump of local contents of memory
- IAESS Common Input Messages**
- Messages always terminate with "end of" ;
- x-number of your network #
- NET-LINE:xxxxxxx0000: Trace of call through switch
- NET-TRK:xxxxx: Same as above for trunk trace
- T-ON:MBxxxxxx: Makes a # busy
- TR-DEACT1-25:xxxxxx: Deactivates call forwarding
- VF-Y-DNA:xxxxxx: Displays class of service, calling features etc.
- VF-Y-LEN:xxxxxx: Same as above for CE
- VF-Y-LIST OS:xxxxxx: Displays stored calling data
- \*\*\*
- There are many things I didn't cover in this article and many of the things I covered I did so very briefly. My intention was to write an article that explains the big picture, how everything fits together. I hope I helped.
- Special thanks to all the nice people, (ie: without them, some of us wouldn't be so smart and might have to work for a living). Also special thanks to John and Dave for writing their guidebook, this would have never been written. Yes, people, there are great hackers out there that no one has ever heard of. You just have to know where to find them.







# IT'S THE

# LETTERS PAGE

## COCOA Troubles

Dear 2600:

I am presently enrolled in a senior high school in Fayetteville, NC. This school is rickshaking its students blind by having two COCOAs in the lobby. I obtained a copy of 2600 through a friend and I am interested in recording more. Furthermore, I would like to request some extra information in hacking out these COCOAs so that I can get free IDs. My friend noted that these phones used a hanging pulse that hung up the phone when it read error volts on the line. So he hooked on a radio volt battery. In parallel with the number connector, I want to see if there are other less difficult ways of hacking this phone.

RM

By all means, figure out how the phone works, but if all you're interested in is making free phone calls, you're not a whole lot better than the telemarketer who stalks the phone in the first place. See what happens after the called party hangs up. Do you by chance get an unrecorded dial tone on your end? Look for speed dials - that one programmed in the line or ground keys. And see what happens when you call it. We suggest reading The Magpie's COCOA guide (Summer 1990).

## Future Surveillance

Dear 2600:

The article "New Revelations from BellSouth" by Kenneth Goldstein, Autumn (1990) describes new monitoring technology. Even this description, it appears to be a well-designed system for performing such monitoring. The author appears to believe that BellSouth should have improved their security in a different way.

However, wasn't the goal of some of the attacks against various Bell computers to demonstrate that Bell should improve their security? Why, then, the objection when they actually do so? And shouldn't they be free to select the method that they want?

RM

Minnesota

As you know that method carries extremely troubling implications. Note that the recording device BellSouth is interested in is capable of far more than "improving security." It can record a variety of lines surveillance by recording voice, fax, and computer

transmission electronically. Its configuration made one to the conclusion that any interested entity will be able to monitor an individual throughout even without the phone company's knowledge or approval. That's something none of us will be spared by.

## Why Did You Do It?

Dear 2600:

I was disappointed to see that you published the credit card algorithm in your Fall 1990 issue.

Although I know it was well within your Press Amendment rights to publish it, I think that it serves no purpose by being published except to leave innocent credit card holders open to abuse by individuals who just wish to call a phone sex line or place a long distance call over an ADS. And although I know that the algorithm was already well known within the hacker world, I don't believe that your magazine should have spread it further.

In previous issues of 2600, you stated that credit card fraud and long distance wire abuse are tantamount to stealing and have nothing to do with the hacker ethic of learning and exploring systems. Therefore, I see no reason to prohibit the credit card algorithm if your magazine truly believes in the above. The only uses of the credit card algorithm by your readers would be to generate numbers to be used to phish calls over an ADS, access to phone sex lines or 800 chat lines which use credit card numbers for billing, or to obtain actual merchandise as the authors of your article state that often credit card numbers are often checked only against the algorithm and then billed later.

Please stick to your stick. If you believe that credit card fraud and code abuse are stealing and not hacking, then please do not publish any information that would be used to those ends. And please try not to publish materials from authors who call themselves names such as "8000/5000 Alchemist". Your mag will end up looking like a "copycat" coder philer.

RM

Minnesota

You make good points, but you missed the point of 2600. We published that information so people would understand how the technology worked. What they do with that information is not our business. Based on

for further questions

Dear 2600:

In the article "An Algorithm for Credit Cards", there was an error in the C code that caused the program to incorrectly determine the weighting factor for 13 digit Visa cards. Here is a correct version, as employed in the form of a function:

```
int valid_credit_card_number(
    int card_number)
{
    char card[16];
    int valid = 0;
    int card = 0;
    int edigit = 0;
    int even = 0;
    int odd = 0;
    int sum = 0;
    int card_number = strlen(card_number);
    int i;
    for (i = 0; i < card_number; i++)
    {
        card[i] = card_number[i];
        if (i % 2 == 0)
            card[i] = card_number[i] * 2;
        if (i % 2 == 1)
            card[i] = card_number[i];
        if (card[i] > 9)
            card[i] = card[i] - 9;
        sum += card[i];
    }
    if (sum % 10 == 0)
        return(1);
    else
        return(0);
}
```

/\* Is this the right length for this kind of card? \*/

return(strlen(card));

case VISA:

if ((strlen == 13) && (even == 16) || (even == 14))

return(0);

break;

case MC:

if ((strlen == 16) || (even == 15))

return(0);

break;

case AMEX:

if ((strlen == 15) || (even == 14))

return(0);

break;

for (i = 0; i < strlen(card); i++)

edigit = card[i] - '0';

if ((i % 2 == 1) && edigit != 2)

if (edigit > 10) edigit -= 9;

even += edigit;

if (even % 10 == 0) return(1);

return(0);

}

This function will return 0 if incorrect. If correct, "VISA", "MC" and "AMEX" are suitably defined constants, and may be spaced. Thank you for including this article — we have learned something to keep people from

hand-signing on card entries.

Kenton A. Hoover

Chief Engineer

Whole Earth Learning Link

## Questions

Dear 2600:

I very much enjoy your magazine and I am curious whether certain companies tell the federal government or the phone companies the names of people that send you for records to make a red box.

Also, please print the frequencies of each touch tone 5 in writing (includes with them).

Bob

Woodmere, NY

We not beyond the realm of possibility but some depends on that. The solution is to do what appears to you and not worry about what others think, whether they be ignorant people or misguided bureaucrats. Touch tones are composed of two frequencies each. Attach your touch tone keypad, with the extra A/B/C/D buttons on the right. Then place the following frequencies along the top:

1200 Hz, 1300 Hz, 1477 Hz, 1680 Hz

From left to right, the frequencies are 600

Hz, 770 Hz, 850 Hz, and 941 Hz. Find the

number you want and combine the two tones

for that number and you've got a dial tone!

## BBS Troubles

Dear 2600:

I have recently used the two articles about the FBI case that were published in the Spring 1990 edition of your magazine. First of all, I want to thank you for bringing things like these into the open. The federal government is always trying to keep their misconduct (which occurs all too often) under their hats, and it's great to see that people still have the guts to stand up to it.

I have also been feeling the effects of these "watchdogs" here in the Twin Cities. Many a BBS have disappeared (along with their operators). Many more have been looked into, but allowed to remain. Almost every user in the state now posts a warning message about the "prowl" of e-mail. I feel sorry for one BBS in particular: Maricopa. It was already known to everyone that this BBS was completely legitimate. Yet, recently, they were the subject of a federal investigation, apparently they had a sex (of users that were referred to as "jaded" users). Someone who was misinformed and didn't take the



## LETTERS FROM

## AROUND THE COUNTRY

The Concerned  
Users

### Technical Suggestions

Dear 2600:

I got picked up a copy of your zine as Dark Carnival is finally starting the good work. Some comments on "Hunting for Whoppers" (Summer 1990, page 24):

There does not use series voltages, not does Sprint. The analog hybrid line going into your telephone goes into a SLIC (Subscriber Line Interface Circuit) in the exchange, where a chip called a CODEC (coder/decoder) converts it into a digital PCM pulse code modulated stream. This is what actually gets searched in those SFFS searches. Bell likes to talk about it, you are still on the N90, it is a simple matter to order the switch to send you a copy of someone else's chatterbox. This is a wrap-up in software, for all practical purposes impossible to detect.

Unfortunately, most FBI agents know how about the phone system than a dead mule and are equally unable to detect. Twelve volts sounds about right for the weak line while negotiating a conversation, but it's since the 100-150V to operate the bell. The lines have a high voltage rating about 500V (50V below the tele surge suppressors cut in and before that before the SLIC starts to burn. My guess, for the other hand, have a maximum rating of a hundred volts or so, which is why some lines between hunky when they are rapped (falls to ring or fails to answer when picked up, or very poor audio quality).

The best way to test for an over-volt would be to discharge a photoflash capacitor (330 FFW) at 30V volts into the line and look for the bright flash of light as the up surge went to that great transition in the sky. But use some caution, as the capacitor is not a toy. Get a friendly fellow person to unplug the SLIC and plug down the ends of the line with dielectric tapes and do the same with your card. Confine that there is no lightning working on the line or on a nearby one. Then double check. The capacitor is easily capable of killing a human being as well as a fire next to it. Don't connect a 300V power supply directly to the phone lines or you are likely to hurt someone - particularly yourself. Place the voltage off both the capacitor and the line before unplug anything. If you ever

time to have said things further assured that the "privileged users" were hackers and received access to some secret part of the UDS. Actually, a "privileged user" is someone who contributes money to the UDS and receives privileges such as more online time, extra downloads, etc. The operators have since changed the status to "contributors" rather than "privileged users" to avoid future hacker paranoia. It is hard to believe that this anti-hacker paranoia has grown to such proportions that people even get harassed for merely contributing money to a UDS that they host. In any case, I'm glad to see that this board, as well as many others, has survived the attacks and has the pride, determination, caring, and guts to remain in operation.

Finally, show my tutorial to cases such as these how soon recently. I would like to know what else is going on. Here in the Twin Cities, I have been waging a battle of my own against censorship. I am concerned about how successful the PMRC (Parent Music Resource Center) has been in limiting the rights of musicians to say what they feel. Also, I feel that hackers are not doing anything that would cause harm to anyone, and should also be guaranteed the right to the First Amendment. I would like to receive more information about your magazine and how I may subscribe to it. I want to assure you that I am not a federal agent, nor do I have any contacts with the Federal government. I am not interested in busting you or your magazine, but simply in learning more about what is going on.

### The Specter

St. Paul, MN

I wouldn't expect if you were. We probably give some information to anyone who's interested. We hope to see hacker bulletin boards (except from what has been a beards/assessor from what has been a copycat here). There are a great deal that are only underground now. The need for public hacker boards has never been greater. Anyone who has questions about this should contact us.

Dear 2600:

I have been hearing rumors that the Federal Communications Commission is going to begin forcing BBS systems to keep falsified logs of their BBS's up to three years back. As a BBS sysop, I find it good practice to keep my logs, but after all of the work I've put into the board, I don't want the

government telling me what I should do with it!

Charlie Tuna  
Kokomo, IN

This is only one of the many processes being put on system operators. Another is the threat of changing business phone rates to include boards, an action that would put many of them out of existence. Consider these things by making both your users and other system operators. And by sending letters to your publishers too.

### Another Method

Dear 2600:

I just received your Autumn 1990 issue and, like always, I read it cover to cover. Very enjoyable and enlightening. I am involved with month-long seminars for the obvious reason: data reception from satellites, and just about anything else that is beyond the normal grasp. I have the programming procedure for over 45 cellular phones and a complete listing of secret codes for all states, several COCCO payphone manuals, and wiring diagrams. Between your magazine and the UDS Newsletter, I get lots of ideas. For your readers that don't know, UDS Newsletter sells lots of manuals and plans. I have been a fan of theirs for years. I got my alert in CBS and progressed from there. Just thought I would let you know that I appreciate your existence.

Now for the good stuff. Recently I found a COCCO that had the serial numbers on the back mechanisms. It didn't get any easier than that. After opening the phone I discovered a programming switch inside. Now I can remove the clock run to dump the passwords and, to my delight, I now have an opening payload. Just for fun, I left it in the same location, with the passwords changed of course. In reality, not into that. I just like to explore. Dig 88 holes, the programming access code, default is 98. You guessed it, 98. You would be surprised to know how many phones are still in default. And it was definitely using the ANI number supplied by 2600 will yield any COCCO number that is not on the outside of the phone. Call the phone and enter 98. If you gain access, it's fun to play around. Also will reveal all bins to default (except

password, time, and date). 9110 will reveal the rate table bins to 0. 9111 will cover the rate table adjustment mode. Bin 11 is the rate for local calls and Bin 12 reveals the intra rate 11 - seven digit calls. Bin 14 controls the long distance calls. Naturally, I can never go back to the phone's physical location and open it, but it sure is fun to call it. Less than thirty days after I did this the phone was replaced (guess what! The back mechanisms had the serial numbers swapped around).

Mr. T.

### Suggestions

Dear 2600:

In your last issue you had an article on building a telephone and which I thought was brilliant as far as the wording of the red box goes. There is a simpler way of doing this which has worked better. Radio Shack sells something known as a Telephone Hack-up which goes for about \$1.00. This plugs in straight to the "base" of the tape. Obviously, one has to then go to two adjacent phones and do their deed. However, instead of looking for two adjacent pay phones, you can have your number/hacker/buffer/stealer/finder/digger etc. go down in the way phone and deposit the quarters for you while you sit home and receive them on a tape recorder. When required, I suggest using a metal cage for longer duration. Secondly, don't have this type on the car or the sun since it may change the pitch of the tones and AUCS will have a hard time picking it up, and thus you will be considered a failure.

I enjoyed the tone dialer conversation with you tremendously and thought it was a great idea. Keep up the great work.

What I think 2600 should do now is introduce some UDS's. When Central Office and Toll Center were running it was great. The communication between hackers is very important. The next generation of hackers will soon be those to take over and all they will be interested in is "tools". These days the BBS's on the hacker community are generally filled with "welder-riding" kids. No real knowledge is passed on. The Toll Center had means to translate new ones in hacking which was fortunate. Both your bulletin boards are marked, which was wonderful. Now the UDS world lacks such boards to call. Think about it.



# LETTERS FROM

# AROUND THE WORLD

get a idea person to help you out, drop the project. The method is safer than dragging from telephone poles parking at high voltage lines with a stabilizer, but it is still very easy to get someone.

As for getting a 747 with a piston unit (Piston Cessna), Jack Still, a lot of the early portable computers were very big about 700 guidelines for medical PPI. There almost putting a multi phone inside an early Compaq or Babbage and handing it to a passenger as carry-on luggage. Then that up for him while it's in the air and download a few files. The electromagnetic keyboard existed by the 70 could jam the 747 rig by wire antennas. Having the pilots with no control over the phone. If you want a solution, do the feed during takeoff or landing - the 747 will be more likely to hit something. It should be fairly easy for a hacker with a scanner to intercept the dial call, although identifying the guilty party might be more difficult. Perhaps your hacker can read the weather readings and trace the call. Or his girlfriend is a cop and she traces it for him?

## Caller ID Override

Dear 2600:

From what you know about the caller ID systems that are gradually being introduced, do you think it would be possible to build a circuit or add-on box to your own phone phone to send a false number to the party you are calling? It would seem to be the ultimate defense against the invasion of privacy while at the same time giving the appearance of cooperation without a tip for privacy showed up for everyone's caller ID screen.

Peace

Allen, OH

Absolutely. We hope to see someone do this soon.

## A Phone Company Tour

Dear 2600:

I had the opportunity recently to take the 4KSS owned by AT&T here in Cleveland. I went along with a tour offered by the local chapter of the American Society of Mechanical Engineers. It was an interesting afternoon tour of five different levels of technology were present in the same

building. These ranged from hardware, dedicated lines leased by companies and corporations for direct data, or voice communication between distant locations (Bellsouth America can pick up a phone here in Cleveland and immediately ring a phone in the New York office without actually making a long distance call). I gathered that this was a pretty expensive system and would only pay off if you made a lot of calls to the same long distance point. This system was still using the old style silicon-etched boards that were the rage earlier this century.

There were so mechanical switches in use, but there were several levels of electronic switching ranging from large, cabinet sized control boards to the new fiber optic systems that they were set in the process of installing. The whole system was backed up by a mental of massive set cell batteries that would supposedly keep everything humming smoothly for about eight hours after a power failure.

I was surprised to find that there are only 15,000 outgoing long distance lines emanating from the Cleveland 4KSS. I had suspected that there were many times that number since this is such a big area with so many customers. I was also surprised to see small the cable plant existing into the 4KSS from the Government area central office was I would estimate it to be only a couple of feet in diameter and it was entirely unpowered when it entered the building. It hope no nerds are reading this!

The AT&T letters were quite knowledgeable and informative. They seem attempted to go into a little something funny, obviously thinking that a group of mechanical engineers would be appreciative of such information. I was, but my fellow engineers were busy asking questions like, "Is there really a single wire that runs from here to Columbus that you talk over?" and other questions surely require an answer. I was embarrassed for them and for my head in shame.

I totally stuck out in asking questions about the AT&T for this area, and in wondering about why the phone company changes for town come service when the whole thingy system is based on these rugged built boxes. Of course, scoured all available paper for phone numbers, but everything was well hidden. My mouth

watered when I saw the full set of operational manuals for the 4KSS sitting out in the open.

A major screen went off in the system while we were listening to watching theory. It seems that someone dug into a large set of rather important cable checker somewhere in eastern Cleveland, causing cutting three or four control offices off line for a while. The technicians on duty knew what had happened in about three seconds after the printer started dumping trouble codes. One of the guys even let us peer over his shoulder as he accessed one of the downed connections and did some diagnostic checks. Pretty neat, huh.

Well, enough about my little tour. How to some suggestions for future issues: program listings for an IBM compatible computer for a blue box, a red box, and some dialing programs. In-depth searches, extract searches, etc.; non-proprietary listings of exchanges other than New York area; ANI and CMI hash access numbers for the SLS area code; more BBS numbers; book reviews; equipment reviews (computers, pin rigs, etc.); phones, modems, and other things that can be used for hacking and phreaking; more hands-on information; and information on ATM machines and their ilk.

Mike

Cleveland

## Assorted Thoughts

Dear 2600:

In my area, Ma Bell finally improved one of their long distance nodes: they got rid of the operator for night calls. One can no longer bill to another number or make a collect call with a human operator. Instead the system will ask for your name and digitize it and play it to the destination to verify the billing. So the person you are billing will probably recognize whether or not the person is actually the one claims to be. It sure took them a while to figure that out.

Anyway, with this procedure one can also make the own local calls have judge pay phone. The good part is that it's completely legal. Just bill the destination and when the system asks for a name, say the phone number of the pay phone. Regularly the person who picks up on the other end has some common sense and calls you back. So now you don't have to carry around any change and you still save

yourself a good twenty cents in fees add up eventually.

By the way, Sprintnet (also known as Telenet) is doing some sort of deal with transmitting data in printed form to addresses via 05 mail. Does anyone happen to know how to access it? I'm trying to through a net but the too expensive. The pretty sure there's a way to do it cheaply.

## Keyboard Stealy

Call 800-TELETYPE and ask them about that service. My local has something similar if not identical. You can always use an operator for odd or third party calls if you don't have a home fax phone or if you say you don't.

Dear 2600:

I really don't want to write another one of those "Gee, I really really like your magazine..." letters, but unfortunately that is exactly how I feel. I am in my mid twenties and say, say, based on the silicon dark ages (put it this way, I can remember when the 7004 IC was thought by some to be ahead to the part that would never exist the night it was the market leader) I discovered computers and modems. I had a second-hand Apple II which I still use with quite a bit some other hardware. enhance current. A Hayes Keyboard II (I guess upgraded to a Practical Peripheral 2400) eventually, some "terminal" software and a lot of native curiosity, I saw how a "hacker" per se, since I have about a third grade computer literacy level and the notion of my hardware knowledge is knowing what wire plugs to where, and I did do some things on that dark time right after the breakdown of the phone company. That same winter under the coexistence tells me were not overwise, but I really didn't know any better.

With my little boy I discovered a whole new method of communications, with the immediacy of a telephone call and the depth of a letter to the editor. It also opened up the world of encryption technology. I looked about the catalog of boxes that remain private now to test the limits of the phone system that 50% percent of people (myself sometimes included) take for granted. I heard about different computer systems and how to get into them. Finally, the never really wanted to hack myself, but it's always been fun to find out how I could do it, and stories from those who did such things were always fun to read.

In short, I experienced what the business



# LAST OF THE LETTERS

## COCOT Info

Dear 2600:

of the U.S. Constitution had hoped so when they set down in Philadelphia in 1787, the first real open exchange of ideas (no baron from WASCO's Bob Grand). Even if the information should a little to the good, it was still harmful. You, freedom seekers, you have to hand it to you and her to do what you wish, eventually the carrier of the freedom may impinge upon the freedom of someone else. That is why we have laws, some fair, some not. Now, I'm not saying that laws cause terrorism because there is a certain percentage of humans who will always do things at the expense of other humans, but I do believe that within laws will weaken otherwise latent tendencies in people. Some people will increase their "law-breaking" in the face of unfairness, those in power will resist with tougher laws, and so it spirals up until it can go no higher and subsides in the wake of a social collapse.

What does this have to do with 2600?

Your publication is one way responsible authors have of participating the wilderness in our post-industrial society. Since information has become power in our society business, the traditional publisher that CNS has over government policy, those in power, whether they are government or business, find it important upon themselves to control what people know. Fortunately, we live in a more or less free society and we can get access to information if we dig for it. There is enough self-educating information spread across all of the U.S. government's own pamphlets and press releases to keep self-appointed "government watchdog groups" in Dallas, Bethesda, etc. but that information is not published. So maybe the key to our so called "Information Economy" is publishing. Sure, IBM gets all the publicity for marketing a long-child, hard-to-use computer, and Apple Computer can give the details and Macs of computer users, but who outside of search-and-reports computer buffs know about the Amiga, or even Steve Jobs' reality? They can blow IBM power users' dream machine, but who's really heard of them?

So this time the "Information Age" is the "Publishing Age" as Adolf Hitler said, if you raise the veil the most outrageous lie you own. The answer is better that way.

The Disco Strangler  
South River, NJ

Dear 2600:  
This is just a little something interesting we've discovered. The phone numbers (both in the 212 area code) are the ones which appeared as a response to a letter about the article on COCOT's which appeared on page 81, Summer '90. The two numbers connect at 305 head and send the following alphanumeric strings:

- 212 265 6129
- 198\*2122086129\*41465\*CA2203\*6837\*1
- 43\*010116171141\*XX\*0000
- 212 265 6129
- 798\*2122086129\*41465\*CA2203\*6837\*1
- 43\*010116171141\*XX\*0000
- 212 265 6129
- 798\*2122086129\*41465\*CA2203\*6837\*1
- 43\*010116171141\*XX\*0000
- 212 265 6129
- 798\*2122086129\*41465\*CA2203\*6837\*1
- 43\*010116171141\*XX\*0000

The Muffler and  
The Mule & Bach, Inc.

Now this is where we like to see. Besides being a user themselves to go further with the information we give. Is there someone who can explain what these numbers mean?

2600 is always in need of writers!  
If you've got a field of expertise or a story to tell, send it in to:  
2600 Editorial Dept.  
PO Box 99  
Middle Island, NY 11953  
Questions?  
Call (516) 751-2600

ORIGIN

# MAUGKS

50g

FOR THROAT & CHEST

HOBSTBONBONS / BONBONS POUR LA TOUX  
HOBSTBOCHT / BOBONBONS

CAN YOU BELIEVE THE THINGS PEOPLE SEND US?



# OUR CONTEST

In our Summer 1990 issue we published a bunch of negative letters that were written about hackers. We invited our readers to come up with replies. The winner would get a free Marlowe subscription. We got a pile of really good entries. And when the dust cleared, we realized that we had two winners. Unfortunately, neither of our winners did a very good job of identifying themselves. So we have absolutely no idea where to send the subscriptions. If you recognize your name below, contact us and mix of some way to validate your identity.

## Entry Number One

by TELEPODZIS

I found the Summer 1990 issue very intriguing - particularly the section dealing with the other part of view against those who attempt to learn more about systems. As I was reading these letters of anger, there, and disgust, I was struck by how similar this situation is to what Dr. Richard Feynman experienced during the development of the first atomic bomb.

In the book, Surely, You're Joking Mr. Feynman!, there is a chapter relating how Dr. Feynman was able to crack open U.S. Army safes which held the plans and drawings of the then being developed atomic bomb in Los Alamos (chapter entitled "Saboteur Meets Saboteur" - pages 119 to 137, Bantam Books). Feynman had discovered, after speaking with a saboteur, now most safe technicians give a standard assigned combination number to safes, instructing the buyer to reset the locks. Most buyers, however, didn't bother reassigning their safes with new combinations, failing to realize that the standard assigned number was just that - a standard assigned number for all safes then being made. What Feynman did was go around and open the Army's safes within the Los Alamos compound (he was able to open one out of every five) with little trouble for nobody had thought of bothering to change the combinations after the safes arrived from the factory!

How was Feynman treated? With respect and understanding? On the contrary, he was nearly thrown out of the Army change the safe combinations? Sure eventually, but not until after several months into the project.

So you ask yourself - what the hell was Feynman doing? Couldn't he just leave well enough alone?

No, Feynman had a curiosity - the very same curiosity which led him to develop new and better understandings of the atomic sub-structure led him also to find ways in which to open up Army safes.

This is the crux of the argument and controversy surrounding hackers: people are actually curious. Trying to stop this curiosity from enveloping the world around us is akin to trying to stop a mountain of water. Even if we did, it'd only bring about more trouble (besides developing new and wild forms of nervousness, for men is differentiated from animals on many points and chief among these points, curiosity runs the pack.

It's fascinating, but none of these letters spoke of harnessing the very same curiosity and drive toward protecting their systems. Instead, we all merely throw things about, rant and rave about how terrible it is for people to go "walking through their house" without stepping and considering how to find out ways of positively utilizing the skills and powers of those capable of doing so.

But an even more important point not being raised throughout any of these discussions is the fact that perhaps privacy is nearly dead - and it ain't by those kids. When you stop and consider how many files the U.S. government has on each person - whether you're in the armed forces, receiving or have received a college loan, possess a driver's license, hold a social security card, maintain a farm or grocery store, pay taxes on a regular basis, the list of the matter is that there are bigger and more nasty people who manage through your house on a regular

# WINNERS

base - and you don't even realize it!

Protection of our credit records is probably one of the greatest non-issues today. TRW or Durn and Bredtreat regularly sell information on your credit status and income standing to corporations which seek out to find new markets to sell their products. It's a part of rule that every time you receive junk mail, somebody assessed your credit records.

And we're worried about punk kids taking a walk through telephone companies to get information that they could receive by the mail for \$13 - as the Neiderf case proved?

Somehow the real criminals are getting away scot-free.

I respect people who take the time and effort to find ways into computer systems, for we all learn much from it, it keeps us on our toes. And in the spartan society I also feel better when I know that there are people who do care about the world around themselves and take the time and risks upon themselves to learn more.

That's not only curiosity, that's entrepreneurship. Equality is never something given; it is only achieved and maintained through diligence and persistence. Having information hidden away is antithetical to democratic freedoms. Seeking out information makes us grow and become more competitive on the world market; this is what makes our country great.

As a professional operative, I think many of these people would be mildly shocked if they found out to what extent and degree private and public institutions employ people such as myself, and how much information is constantly available on the average citizen.

I have little regard for those who brand "hackers" as threats for no other reason than for their impassioned curiosity. Grow up yourself! This is a bigger world than you realize and, as a professional, I frankly find this talk of eager to be utterly misdirected and somewhat naive. Attack TRW, Exxon,

the Republican Party... Any corporation - public or private - possessing of multi-faceted interests is inevitably going to have some sort of computer system and with that system are those who are going to make sure that it works - even if that system is meant to take information about your checking account, car insurance payments, psychiatric care, or even if you had recently purchased any Elvis records!

It is not surprising that the majority of these hackers are young. We should come (and pray) to expect more of these individuals to arise no prominence, for we are a country that is losing touch with its people, most particularly its youth. Have we stand, bitterly complaining how many youths cannot read a map (much less actually read) and yet we have those able to discover new means of accessing information which even the so-called "experts" never realized existed!

We are quishing talent that this country desperately needs, rather than reaching out to exert this raw and excellent energy into new and vital means beneficial to all - particularly those who possess this great inner strength.

No, don't go for the kids who runnige through your garbage; go for the faceless professional bastards who keep and maintain a detailed profile on you so that they can sell you watches, cars, beer, and, yes, political issues. For it is they - those who maintain those giant mainframes without even bothering to think about the consequences (as well as those who ruin) that we should be watching.

The child who discovers that the emperor is nude should never be punished. It's time that we start noticing these little details.

## Entry Number Two

I'm a hacker. I worship the computer and the endless possibilities it poses. I see programming as an art, and I was born to explore. When I sit down at my computer to do something, I don't debate in my mind whether or not what I'm doing is illegal or



## IN DEFENSE

unethical. I just do it. The computer is a medium which is so immediately exploitable, with a scope so infinite and a depth so limitless that it makes just doing it extremely feasible. That being the case, there is more to a computer than programming, and those with an insatiable interest to learn and know easily assimilate themselves into the abundantly available aspects of the computer world and, inevitably, into aspects associated with underground activity. This type of person, the hacker, does not think in terms of right or wrong, as the definition of these terms depends on how you look at life in general. The means is the ends, and the ends justify the means. Columbus was a hacker. He explored new worlds because they were there. He didn't stop to wonder what effect his discovering the New World would have on the Native Americans. He just did it.

Leonardo daVinci was a hacker. He explored the human body, among other things. In his time, it was forbidden by the church to dissect dead bodies to find out what made a human tick, but he couldn't care less what the church had to say about it. He had a desire to know, so he just did it. Humanity has a history of wanting to know and this desire to know sometimes leads to questionable means. Questionable, depending on how you look at it. If it wasn't for the hackers of different sorts throughout history, where would humanity be now? Although we probably wouldn't still be dressed in animal skins if people had always remained congenial to those in authority and shied away from those things that we "weren't supposed to do", we wouldn't be as readily advanced a civilization as we are today, it's because of those people who dared to know and had the desire to understand the world around them that we are at the point in history we are today. We owe a lot to hackers.

Although I'm not a gun-tho systems hacker, I've done enough to understand the thrill and slish the challenge. I was once under surveillance by the phone company

for being where I shouldn't have been, so I feel I'm at least that much more qualified to comment on this subject than your average Joe computer user. It's called experience, and that's something I have a fair amount of due to that peculiar instinct we all have inside of us called "hacking".

Some people believe that when you hack you are going somewhere you do not belong and equate this to breaking into someone's home. This is a stupid analogy that is much overused. Hacking is a game as much as life is a game. If you choose to play, you accept the risks associated with it. If you win, you win, and if you lose, you lose. What are the rules? What are YOUR rules? You play the game as you wish and you deal with the consequences as they come, and only your conscience and personal integrity dictate where the game leads.

Scenario: You break into a house and you start looking around for something interesting that will tell you about the owner. Many things can happen at this point, one thing being the owner of the house wakes up and finds you rummaging through his file cabinet, whereupon he pulls out a .357 magnum and bows a two-inch hole through your chest and you die.

You can see how the analogy between hacking into a system and breaking into someone's house doesn't hold up too well when you really put any thought into it. When someone goes through the trouble of breaking into a home it is usually for malicious intent (i.e., to burglarize, rape, etc.) and rarely just to dig through personal files (which is not the definition of hacking anyhow). Hacking is something you do casually in the comfort of your own home. With the majority of hackers, there is little likelihood of any intent to do harm, but rather an innate curiosity. Can the same be said of a burglar or a rapist walking into an unlocked home? Someone breaking into a residence usually has premeditated a crime. A hacker is merely exploring. It is the process of exploring, a very tempting bit

## OF THE HACKERS

of information is found, the hacker must make a decision: does he download the file or leave it be? If you go to buy a newspaper from a machine and find that the last person to purchase a copy left the door open, do you take a copy without paying for it? Nobody would probably ever know if you did or not, so the question comes down to your personal ethics. Do you take it or leave it? What are your rules?

Scenario: This strange system you've just hacked into turns out to belong to one of those mailing list companies that sells your personal information to those annoying sweepstakes and mail order firms. Is it alright for them to sell your personal information and for you to be looking around in their files? Is it wrong for them to be selling your personal information as well as for you to be looking around in their files? Neither? Either? Both? What are your rules? They're making money, which they enjoy, and you're learning the system, which you enjoy. Are they wrong for wanting to make money? Are you wrong for wanting to learn? What are your rules?

Now let's say you've done something particularly heinous, such as broken into a Bell South computer system and deleted some file called something like "E911 Overview" which is purported to be worth around \$79,449 (actually, \$13 with a \$79,436 legal fee). Eventually the all-powerful and all-knowing Secret Service, that institution of unfathomable intelligence, tracks you down and decides to smite thee and all in your path with its mighty wrath. Well, now you've been caught. You played the game and landed on "Go To Jail", and you ain't passing go, baby. You took the risks and lost... but the game is more complicated than that.

Since we all have to participate in this game, whether we like it or not, it is necessary to explore the effects of this broad-scope action taken by the very government institution which we entrust to protect our God-given rights. The minute

details cannot be ignored, as they are the scariest and speak the loudest in terms of criminality and injustice. Yes, even more so than that evil 15-year-old punk with the ego.

This treasure dubbed the "E911 document" makes its way through numerous systems via a network, unbeknownst to the owner of each particular system. The SS (Starbuck Troopers), while tracing this document's trail, come across one system that the document made its way through. To them, it's obvious that this system was involved in this plot to defame the emergency phone system and lead to the downfall of the government, the country, the world, and then eventually life itself. So they see no problem with contacting this system and everything else that looks suspicious inside the globe where it dwells: the disks, notes, books, magazines, music tapes, stereo, TV, lamp. No, not even the toaster is immune from this rampage. Hey, it's got a cord on it, it must be involved in this devious scheme somehow! Maybe the person being stopped of all his possessions and dignity at this moment, who in all likelihood is being physically restrained by four men in dark sunglasses, his poor mother in handcuffs with a double-barreled shotgun pointed at her head (she just might try something, you know), is some undiscovered super-genius who has developed a method of encoding data on toast. They want to check these bread crumbs at the bottom just in case.

Scenario: Someone who has just burglarized a home runs through your yard as he attempts his getaway. The cops trace his trail through your yard. Are you now guilty by association? Do the cops rampage into your house with destructive force, confiscate all your possessions and terrorize you and your family members so gather evidence that proves that your neighbor's house had been burglarized? No, is this analogy more suitable than the one so cursorily overused by those who



# the word

We've published information in the past on AT&T's HISA Direct. One of business, we should tell you that there are other similar services that allow you to call back in the United States from other countries without having to deal with local operators who often don't have the common decency to speak our language. You can now avoid foreigners on the phone by using Sprint Express. You'll be conversant with a Sprint operator in the United States who won't disappoint you. Some countries and the numbers to call from them: Argentina: 001-800-271-1111; Australia: 0014-881-877; Chile: 001 for 100; 0057; Colombia: 980-14-0010; Denmark: 8001-0877; France: 19, wait for tone; 0087; Hong Kong: 068-1875; The Netherlands: 001-0229119; Japan: 0039-4-331; Singapore: 800-8877; United Kingdom: 0800-891877. All of these connections are toll-free. You can still call to a FONS card, call collect, or use your local calling card.

There's also a new Sprint service that allows you to conference calls. It only works on FONS card calls and not on 1033's or 950-1033 calls. When connected to a call, hitting a star for a full second will put you in conference mode. You can then dial 12 which puts the first call on hold. Then you dial the area code and number of the second call. After the second call answers, you hit another star for a full second, then dial 13. The second call is now linked to the first. If you want to disconnect the second call without linking it, dial 14 instead of 13. There's a 75-cent surcharge on top of the regular FONS card surcharge (since you) on top of the charge for the two phone calls. Maybe somebody they'll finally get it right.

Albert has a whole host of services they've been introducing. By calling 800-783-1444, you can place calls by dialing 0 plus the number followed by your Albert calling card number. Or you can dial a two-digit "Speedial" code followed by a star and then

your calling card number. This will connect you in a variety of offices, hotels, and other rental establishments, all of which have toll-free numbers already, so you'd have to be kind of crazy to spend 20 cents a minute using this service. If you hit a star after entering Albert's 800 number, then enter your calling card number, you'll be able to access InterReach (unrecorded arrangements on the stock market, horoscopes, sports, entertainment, and international time and weather ending between 30 cents and 70 cents a minute). Call Delivery (for \$1.60 you can record a text message for immediate or future delivery to any phone number in the U.S.). Voice Mail (with a 7-digit ID number and a rate of 38 cents a minute), and

ElectronicTime (\$2.00 for the first minute, 49 cents a minute for each caller). In its finite structure, Albert urges its customers to "know or share" and save. What does that mean? It's (other frightening, actually. It seems that Albert now charges calls from the moment they connect the Albert dial tone. (They swear they won't charge you for uncompleted calls.) Albert says, "When I was in hear every word of a prompt or the end of a tone before you continue dialing. If you know the next step, start dialing as soon as you hear the beginning of a prompt or tone. If saves time, plus you won't be charged for time spent listening to instructions you don't need." This is the first case we're aware of where a long distance company (usually admits charging its customers for the time they spend dialing the call.

Albert also has an international call back service. Use U.S.A. Direct and Sprint Express. They call their Option USA. The countries and numbers are: Australia: 0014-800-1125-197; Belgium: 11 8671; Denmark: 8001-0958; France: 05-80-2919; Greece: 00603-15-2100; Hong Kong: 800-8158; Israel: 00177-150-1067; Italy: 8678-97038; Japan: 0031-12-2458; The Netherlands: 06-0128492; Spain: 900-99-1480; Sweden: 020-79-9034.

# in the street

Switzerland: 046-05-8812; and United Kingdom: 800-89-2985. Canadian car access Albert by dialing 800-955-1444.

With all the fussing and fighting in this country over Caller ID, it's interesting to note that British Telecom refuses to provide the service. While privacy may still hold some appeal over there, so do slip-offs. Several companies have sprung up offering CLI (Caller Line Identification) services even though it's technically impossible since British Telecom doesn't pass along the number of the calling party. So how do these companies manage to make these offers? Their devices simply ask the caller to enter his/her phone number before the call is completed. In and behold, the number that the person entered is displayed on the called party's regional device as soon as the phone rings. And the person can enter any number their heart desires. In other words, this is about as far from Caller ID as one can get.

According to an internal SYNEX memo, the system known as COSMOS (computerized) and TRAKS (trunk assignment) will be replaced by the new Bellcore designed system known as SWITCH. It's time to take advantage of the advances made in computing technology over the past 20 years, say the people in charge. SWITCH, which stands for absolutely nothing, is scheduled to follow in late 1991, with implementation to follow a year later. The new system is actually divided into two parts: SWITCH is the "provisioning" part of COSMOS and will require synchronous terminal access, whereas FONS, the dynamic work management part of COSMOS will require asynchronous terminal access. All current COSMOS users in NYNEX and its children (New England Telephone and New York Telephone) will be getting a "network terminal survey" to evaluate the needs of the future. SWITCH was first mentioned in 1989, a while back but it now seems close to reality. We imagine similar plans are being made all

around the country.

According to the Australian (NY) police department, a former resident "boven for causing mayhem with telephone and computer lines" has been connecting their phone lines to the police. "We pick up the phone and we've got the Los Angeles Sheriff's Department on the other end," they say. Newspaper reports claim the villain is able to gain access to the "telephone computer system and use the police department's access code." The translation of this is that he/she is able to get and use a calling card number. According to a friend of this nasty person who contacted 2600, the police have "pursued my buddy for years. Now there's a war between [this person] and the police... for over two years. My friend is a notorious hacker."

If you're a gang member in Los Angeles, you may get to take part in an exciting new technology experiment. Whoever there's a hint of trouble in the area (gang wars, real-estate snafus, etc.), known gang members who are also on probation will be placed under electronic house arrest. These subjects will have created a "personalized template" by repeating the names of 25 states three times in succession to a computer. The computer will then call the gang member at a random time and ask him to repeat eight states. If he doesn't pass, it will call back to give him a second chance. If he fails again, the computer calls the probation officer's beeper. And according to this, don't most gang fights take place late at night? If a gang member has to stay home instead, maybe he'll want to go to sleep at a normal hour. But how can he when he's going to get a phone call from a computer? Also, what happens if the phone is busy? Is using the phone going to be illegal during house arrest? Will calls waiting become "condemned"? And what if the gang member is using a payphone? Will calls forwarded be



## news from

illegal? And what happens when a clever gang member mounts a voice recognition system that is able to generate a response in his voice when it hears the name of a store?

The tech is also coming to the rescue of police/formal relations. By dialing into a computer system called CASSIE SX-4, informants can leave messages for their police contacts. CASSIE will then page the police officer, Ross Distributions of Elgin, CA claims the system will provide more security because "only the officer knows his password". For \$4000 you can get software that can handle up to 75 numbers. You'll still need an AT compatible computer. For around \$15 a month you can get a single line voice mailbox through the Yellow Pages that does basically the same thing.

The next time you get all frustrated at a payphone, think of this: the cost of a local call at a payphone in Poland was recently raised to 20 stajys (just less than one American cent). But 20 stajys coins have become a scarce commodity since they're in such demand. There are two other sizes of 20 stajys coins that can be found quite easily. But they don't fit into the phones. There's also a 30 stajys coin but that doesn't fit into the phone either. So what do people do? What else is there to do in Eastern Europe? Just make use of the black market! There you'll find all the 20 stajys coins you need — at a cost of between 200 and 1000 stajys apiece.

Illinois Bell is applying for Caller ID. The following concepts come from the December 1990 issue of Illinois Bell's Telecraft newsletter: "Illinois Bell believes that a person who receives a phone call is entitled to the same information as the person who makes the call, namely the phone number of the person at the other end of the line. Illinois Bell is proposing to offer Caller ID without the blocking feature that some groups have proposed. With the blocking capability,

abusive callers would be able to prevent their numbers from being displayed, thus diluting the benefits of Caller ID.... What if it is necessary for individuals to establish their anonymity, operator assistance, calling cards, public phones, and cellular phones can be used." What they don't seem to be taking into account is the fact that abusive callers can take these very same steps to obstruct their anonymity. Since it's technically impossible to identify someone who uses the above methods, why few abusive callers will continue to dial direct. What leads us to believe that, despite their sales pitch, Illinois Bell is really interested in Caller ID? It's the non-abusive calls. Of course, if they phoned it that way, people might just think twice.

New Jersey Bell has really pulled one over on the public. Remember when 900 numbers first started being dialed en masse? New Jersey Bell and most other local phone companies told us one way or another: it was easy to block such calls and it didn't cost anything. Now if you want the privilege of not being ripped off by 900 number 700 numbers you have to pay a one-time fee of \$2. Then there's another one-time fee of \$16 to possess the code! Businesses have to pay even more. In all likelihood, less than ten keystrokes are required for the whole order. It's bad enough to see so much obnoxious going on in the phone business, but ripping you off to protect you from being ripped off is more than most people deserve.

Some Bell's statistics: More than 99 percent of the \$8 million calls made every day get through on the first try; about 90 percent of calls to "directory inquiries" get through on the first try and seven out of eight of these are answered within 15 seconds; ninety six percent of Bell's Telecraft's 55,000 public telephones are in full working order at any one time and, on the average, a "hang on a tick" will occur only once every 83 years.

## our exciting world

According to British Telecom, "Nearly 11 million customers are now connected to local area networks, and more than 70 percent of customers are served by modern digital or electronic exchanges offering faster connections, clearer lines, and fewer call failures... Unfortunately there are cases where we fall short of the high standards we set ourselves. To put things in perspective, even if we fully satisfy 99.9 percent of our 25 million customers, we will still have 25,000 who are disappointed."

The British have it so done away with another change that we in the States still contend with. There are no longer connection charges for customers who take over an existing telephone line without a break in service. In other words, if you move into a house with a phone line already installed, you won't have to pay for the phone company to switch the account to your name.

A couple of other British habits from phone company publications: "Think before you dial" is a compelling notion of people getting the most from their telephones. Almost half of British Telecom customers have digitally connected homes, but few know, or try to find out, how to take advantage of all the phone's functions. For example, the cost of BT's operator alarm service has doubled from 1.20 pounds to 2.47 pounds but for just 1.50 a call you can programme your phone to wake you up. Simply pick up the receiver and dial "star 55 star" followed by the three you want; using the buttons on the phone's tone pad for hours and minutes. To check you've got it right, press "star gate 55 gate" and the exchange's synthesized voice gives the alarm time. To cancel the alarm call simply press "gate 55 gate". BT still is not used in the UK. The letter recently appeared in the Sun: "British Telecom services have improved immeasurably since it cast off the shackles of state ownership. We may not like the new telephone boxes, but at least they work. The

company still gets complaints, but at least it responds to them. So we hope it will. Enquiries: BT is now keeping up profits at the rate of 8 million pounds a day. It has a duty to shareholders. You must not forget that although it is a private company it is still supposed to be a public service."

About the most useless thing we've seen in a very long time is the AT&T Callers Club. It comes in the form of a sample of monthly demanding attention. "You've already earned your membership just by being a great customer. How's that? Well, more you need to do, and no strings attached." There also seems to be virtually nothing this "club" has to offer. There are precursors of "surveys and discounts for new AT&T products." Like "VoiceMail, AT&T's messaging service that we wrote about last issue. We doubt AT&T would call "non-members" about their new services and so far we have yet to see any discounts that could be obtained in the real world. We're also sorry to announce that "AT&T sponsored events" in our area. Wow. Unless that includes harbor raids, we're not impressed. A chance to win "treasure prizes" and "valuable savings". Again, nothing we haven't heard before numerous times. Finally, a toll-free number reserved for "members only" (908-223-2000). We can use this exclusive number to "find out about discount periods and calling plans, receive time-share credit for negotiated calls, ask about your bill, get prices for the cost of a call between, specific locations, order your AT&T card, learn how to access AT&T when you're away from home, and notify AT&T when you move, so that you can continue to receive your Callers Club benefits without interruption. We are disappointed. There is nothing here that you can't already get by dialing customer service (800-222-0900) or your AT&T operator. We don't know what AT&T is up to with this gimmick but we'll keep everyone informed. By the way, they will ever give a



# 2600 Marketplace

## To Our New York Telephone Customers

### Beware of Telephone Fraud!

Recently some unscrupulous people—posing as security officers from New York Telephone or other telephone companies, or identifying themselves as federal or police investigators—have tried to deceive and cheat New York Telephone customers. With the excuse of helping them in their "investigations," these "agents" ask you to accept the charges for phone calls from people that you don't know and in some instances they even threaten law suits or suspension of your phone service if you "don't cooperate."

Please, DON'T FALL INTO THIS TRAP. Don't let strangers charge calls to your phone number. New York Telephone is not asking for its customers' help in catching crooks.

**DON'T BE FOOLED** by these impostors that have nothing to do with New York Telephone. If you have questions or doubts, call your New York Telephone Business Office at the number that appears on the first page of your telephone bill. We're here to help.



New York Telephone

A NYNEX Company

We're all connected.

WE DON'T KNOW WHAT'S GOING ON, BUT RECENTLY EVERY CUSTOMER OF NEW YORK TELEPHONE GOT THIS NOTICE:

**2600 MEETINGS.** First Friday of the month at the Clatsop Center—10am-5pm in the lobby near the payphone, 153 E. 53rd St., NY, between Lex & 7rd. Come by, drop out stickers, ask questions. Call 516-751-2690 for more info. Payphone numbers at Chicago 212-229-9011/212 223 8927, 212-306-8244, 212-306-8162, 212-503-8184. Meetings also take place in San Francisco at 4 Embarcadero Plaza (outside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-508-9803/4/5/6.

**BBS/RACHM/R/WRTTR** seeking users interested in credit bureaus for stock or property issues. Please call 301-702-1009 after 9 pm, ask for Edward or write: 131 Dallas Drive, Temple Hills, MD 20748.

**COCCOTS FOR SALE.** Perfect working condition, removed from service. Credit card only type, has good reader built into unit. DTMF, 12 number speed dial.

\$89 each plus \$15 shipping. Call to write for info. Bill Rogers, 2030 E. Chestnut Blvd., Las Vegas, NV 89104. 800-968-8501. (702) 582-7318.

**PALCON** would like to trade knowledge and codes with other hackers. Also interested in raising the barst vidoe, music, etc. Salem, PO Box 1038, 7550 BA, Hergens, The Netherlands.

**CONTROLVERSAL DTMF DECODER** as shown in the Spring 1990 issue. Exclusive offer to 2600 readers: complete revised plans with layout and explicit instructions for construction. Information and hardware currently sold for \$88. Sending a SASE (with .25 postage) nets you 2 pages of info for the slingshot! Laserdisc chip and PC board available. W.E.D., PO Box 273-11, Spring Valley, CA 91976.

**ANTI-WIRETAPPING** bug detection, privacy protection, information services, new and used equipment. State of the art equipment beyond today's technology? National

**Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.**

computer search system, information research service, Radio Shackable, surplus and computer-related equipment. Call E.C.T. Free consultation hotline: (516) 929-3283.

**LOOKING FOR SOMEONE** to correspond with to get a basic understanding of hacking and phishing. (I am in prison.) As I would like to ask questions, please write me directly. If you wish to use a nickname that's free, just make sure you write it as you return addresses or it won't get to me. Victor Mendonca, 9601 NE 24th St, 410216, AnnArbor, TX 79107-0601.

**OLD TAPES** of telephone recordings, tapes, tapes are wanted for radio programs. Also, structural recordings and binary phone calls welcome. Send to Emmanuel, PO Box 99, Middle Island, NY 11953. **WANTED:** Red and blue box phasorbits and assembled kits. Also, expansion cards for a 260K Centaur. Please contact Charles Silman, 11819 Fawcett, Houston, TX 77070.

**TAP BACK ISSUES,** complete set Iss 1-91, high quality. \$56. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatessa, WI 53213.

**TAP BACK ISSUES,** complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. \$100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" \$5 & large SASE w/45 cents of stamps. Peter G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

**WANTED:** Atari ST hacking/telemail programs to trade. I have Stacey Dialer and 2 tone generation programs. N33, PO Box 7516, Berkeley, CA 94707.

Deadline for Spring Marketplace: 4/1/91.

computer search system, information research service, Radio Shackable, surplus and computer-related equipment. Call E.C.T. Free consultation hotline: (516) 929-3283.

**LOOKING FOR SOMEONE** to correspond with to get a basic understanding of hacking and phishing. (I am in prison.) As I would like to ask questions, please write me directly. If you wish to use a nickname that's free, just make sure you write it as you return addresses or it won't get to me. Victor Mendonca, 9601 NE 24th St, 410216, AnnArbor, TX 79107-0601.

**OLD TAPES** of telephone recordings, tapes, tapes are wanted for radio programs. Also, structural recordings and binary phone calls welcome. Send to Emmanuel, PO Box 99, Middle Island, NY 11953. **WANTED:** Red and blue box phasorbits and assembled kits. Also, expansion cards for a 260K Centaur. Please contact Charles Silman, 11819 Fawcett, Houston, TX 77070.

**TAP BACK ISSUES,** complete set Iss 1-91, high quality. \$56. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatessa, WI 53213.

**TAP BACK ISSUES,** complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. \$100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" \$5 & large SASE w/45 cents of stamps. Peter G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

**WANTED:** Atari ST hacking/telemail programs to trade. I have Stacey Dialer and 2 tone generation programs. N33, PO Box 7516, Berkeley, CA 94707.

Deadline for Spring Marketplace: 4/1/91.



TITLE OF PUBLICATION 2600 Magazine, Fall 1990, #133

The above publication has been reviewed and deemed in accordance with Section 2.9 of the LUCR Rules and Regulations for the reason(s) checked below:

- (a) Publication contains confidential information regarding the manufacture or explosives, weapons or drugs.
- (b) Publication contains material that a reasonable person would consider as written solely for the purpose of communicating information designed to act as a hindrance of prisons through inmate litigation such as strikes or riots.
- (c) A specific factual determination has been made that the publication is detrimental to prisoner's rehabilitation because it would encourage deviant criminal sexual behavior.
- (e) Publication contains material on the staffing up and operation of criminal schemes or how to avoid detection of criminal schemes by lawful authorities charged with the responsibility for detecting such illegal activity.

REMARKS Pages 18, 19, 20, 21, 29, 32, and 43 contain information on discussing telephone equipment to make telephone calls illegally and to discuss 4451 and 4452 (Section 11.35911) (Missouri).

If there is a desire to appeal the rejection of the aforementioned publication, this may be accomplished by writing to the Director's Review Committee, P.O. Box 99, Huntsville, Texas 77340. The appeal must be mailed so as to arrive at the Texas Department of Criminal Justice, Inmate/Prison Division, within two (2) weeks of the date shown below.

MAIL COSTS (CONTRIBUTOR'S PAID)

January 9, 1991

Date

2600 Magazine  
 Publisher/Editor  
 P.O. Box 152  
 Mexico  
 Mexico  
 P.O. Box 152  
 P.O. Box 152  
 P.O. Box 152

2600 Magazine  
 Editor  
 P.O. Box 152  
 P.O. Box 152  
 P.O. Box 152

YOU CAN BET THIS WENT RIGHT UP ON THE WALL THE MOMENT WE GOT IT. WE'D LIKE TO KNOW WHAT OTHER MAGAZINES HAVE RECEIVED THIS HONOR. AND HOW MANY MAGAZINES CONTAIN CONTRABAND?

Page 42 2600 Magazine Winter 1990-91

No. 44

FRAUD ALERT

June 21, 1990

**News for the week**

Telecommunications security professionals, members of law enforcement organizations and public prosecutors may not be able to shut down computer data flows if new advocates of business rights have their way. Supporters of Legion of Doom suspects developed a requirement following developments in the highly successful operation Sun Dialer (mentioned here) to only one side-the hackers.

Apparently, the press got late news in 1989 on whether suspects' civil rights had been decided after Louis 123 (we suspect) Mitch Kapor was approached by five attorneys complaining of overzealous enforcement tactics by Operation Sun Dialer, the largest operation of its kind ever.

Kapor, who is president of On Technology, Inc., of Cambridge, Mass., reportedly by contributing \$200,000 to a defense fund for alleged telecommunications. Next, he formed the Institute for Computing Freedom, an expert foundation for hackers' rights.

The highly respected American Civil Liberties Union got into the act after news reports of possible rights abuses surfaced in the Washington Post and New York Times. The result was that a June 5 Congressional Judicial Committee hearing on Cyber 120 matters was postponed so that hackers' rights can be addressed.

Remember that the hacker suspects will have highly articulate advocates at the hearing later this summer.

**Assorted Numbers With Abuse On Them**

- (800)225-0312 (PBX, two nine-digit order; (800)555-4999, one five digit code; (800)326-7900, one 10-digit code; (800)254-6332, three 10-digit codes; (800)843-3313, three six-digit codes; (800)327-8488, one 11-digit code; (800)245-8034, one six-digit code; (800)345-0017, six nine digit codes; (800)562-4656, one six-digit code; Rosemary Newsline; (800)255-9979, box 267 8001; (800)873-5589, a number with high abuse; Rosemary Newsline; (800)758-0123, Phillip Peters, Inc.; (800)444-1533, (800)633-8256, (800)873-5669, (800)877-3444, (800)845-8850, (800)443-4267, (800)273-5966, (800)633-4112 and (800)555-4246.
- Hackers are going after a carrier? (800)586-XXXX.
- PRS: (800)223-5535.
- 950-0511, three six digit codes; 950-1022.
- Director: (800)223-7777.
- (313)950, plus the following numbers: Essex Wheel; 8736 Myrtle; 7068 Park Side; 7538 and 7246 Franklin; 9077; Mischio Man; 6846; Citicorp Plaza; 4586; 514; 7095 (operational code); 9173 and 5610 (SBC's code line); Violator; 8830; 9547 (code line).

Page 409, 5/1990, Communication Fraud Council Association

Page 1

THIS USEFUL NEWSLETTER IS AVAILABLE THROUGH THE COMMUNICATIONS FRAUD CONTROL ASSOCIATION, PO BOX 23911, WASHINGTON, DC 20026 OR 7921 JONES BRANCH DRIVE, SUITE 300, MCLEAN, VA 22102. (703) 848-9768



(Continued from page 39)

ating new penny with all of this garbage — by far the most valuable thing in the package.

By calling 1-900-TSA-RUSH, you can double your fund-raising. Think that you've got a fix on the president? According to the telecommunications magazine TIME, which really should know better, this service "provides every American citizen a personal hotline" to the president of the United States.

George Bush, to comment on issues or pending legislation. "Each call costs \$7.95. The plus side is that you actually get something in the mail: a copy of the fax with a stamp of the president's signature. By the way, if someone can provide us with the real White House fax number, we'll print it. Your chances of actually having your message read by someone will be much greater and your phone bill will be much lower.

MCI has begun offering nationwide 900 service and seems determined to avoid the pitfalls of its predecessors: New 000 services must provide proof that their programs don't violate any regulations or telephone company policies. Advertising will be restricted to make sure it's not deceptive. And MCI will insist that callers be notified of the price of the service and given enough time to hang up if they're not interested. Anything child-oriented oriented services have to be on the same parity as they can be easily blocked.

English Telecom now offers a service for its users in the Persian Gulf to call home more easily. It's called "Uxart Direct" and allows callers to reverse the charges for less than the direct dial rate. A three limit of 30 minutes is enforced to allow as many people as possible to use it. Meanwhile, Military Communications Corp. of Eden Prairie, Minnesota has opened three Proviewers in Saudi Arabia, each of which has 144 Proviewers. They will be able to carry more than 30,000 outbound service and send collect calls every

# the latest

CGI, Military Communications Corp. also owns Proviewers on military bases throughout the United States. And AT&T has set up a toll-free number for families that are having trouble paying their phone bill because of calls from Saudi Arabia (800-223-HELP).

In light of the recent AT&T failures where massive amounts of callers see unable to get through to 800 or 900 numbers because of computer problems or cable cuts, the gettous in marketing have come up with a solution. "Alternate Number Translation" would score the customer's 800 or 900 number into a nearby database. Then when AT&T's system fails yet again, AT&T would use the nearby database to complete the calls. For \$800 per number per month (plus a \$500 setup fee), AT&T will try to keep its failures from affecting you. We'll be trying to get out the names and numbers of everyone who agreed to these terms so we can try to get some free money too.

If you're interested in a worthwhile 800 service, Cable and Wireless seems to have the best low-cost system. For \$10 a month plus call, you can have your own 800 number. For \$21 a month plus call, you can have a programmable 800 number. This is a great service for those of us who move around. Simply call a special 800 number, enter your code, and you can program your 800 number to forward anywhere in the country! The cost of the calls themselves are higher than direct dialed calls, but not by an obscene amount (and far less than calling card calls. We think this is very useful for those of us with imaginations.

Imagine what would happen if some rich entrepreneur-tycoon set up a 800 number to forward to the White House! All of a sudden, every poor person in America would be able to get their opinion heard. (The White House doesn't accept outside calls nor provide any 800 services.) Technology in the hands of imaginative people can do wonderful things.

# developments

Here's a reason to stay off the phone. Remember Telespace, one of those companies that occasionally shows up on your phone bill asking for huge amounts of money for 800 numbers? Remember NTS, one of those companies that occasionally shows up on your phone bill asking for huge amounts of money for operator-assisted calls? They are now gone.

NYNEX is more than a handful of companies; it is a family of people. We must be an ethical family. The only behavior that is appropriate for our businesses and for each of us, is behavior that meets our high ethical standards. There can be no compromise." So begins an internal memo from NYNEX encouraging its employees to get on each other by calling 800-473-TALK from 9 a.m. to 7 p.m. After that they can leave a message on their portable voice mail system at the same number.

Kevin Mifflink made news again when he was barred from attending a computer symposium in Las Vegas last autumn. The Digital Equipment Computer User Society says it never had a known laptop computer register for one of its symposiums before. Their systema fits right in with the needs and government takeover of Mifflink as the biggest threat known to computers. In retrospect, the critics Mifflink was convicted of seem grossly out of proportion to the sentence he received: a year in prison, some of which was served in solitary confinement and without access to a telephone. This unfairness, along with Digital's part in the spectacle, will hopefully be soon over as they are shown rejection of short-sighted individuals who let fear prevail over common sense.

Hungary is the first Eastern European country to get 800 service to the United States... Annettschek, NYNEX, and BellSouth have all been granted permission

to offer electronic telephone directories. It could be a great service if the cost is kept to a minimum ... BellSouth's Bell is offering an electronic directory service called Directics. Customer for large businesses. Each record of information costs 9.2 cents and the charge for a user ID is \$8.80. Oh yes, there's a new from establish cost free of 34752. (The service is located in St. Louis and is accessible via dial-up. AT&T will soon be offering the same service and it will be called "AT&T Field Address" ... Despite a lot of publicity, Pacific Bell's Message Center service can't seem to stop crashing. For the second time in a week in December, the "alternative to an answering machine" went down causing thousands of people to lose their messages. For four hours in the middle of the day, users couldn't access the system at all. Pacific Bell is still proud of the service, saying it "suddenly failed a few times "not causing but 2 and to 3 am kinds of outages". We don't know where they're carrying them but we want to get out of an "answering machine" that goes down for maintenance whenever it feels like it.... BellSouth claims to have become the first of the regional Bell companies to be completely electronic. No more overhead, no more steps... According to The New York Times, Bulgaria has become the breeding ground of "the world's most lethal computer viruses". "Not only do they produce the most viruses, says a virus expert, they produce the best. Why is that? Apparently, a generation of Bulgarians has learned how to program but has no way of using their skills in society... New York Telephone will soon be testing a "debit card" at New York City payphones. Money will be taken out of your bank account as you talk.

Too risky to mail? Then FAX it! 516-751-2608



## DEFENDING HACKING

(continued from page 35)

have little or no understanding of what hacking is? Yes. Instead of being frightened by tall tales of hackers invading your privacy and sifting over satellite transmissions and shutting down emergency phone systems, etc., I'm scared stiffers over the fact that the government can kick my door in and take away my beloved computer because one day I called a bulletin board system that happened to be under surveillance for some random reason, or someone unloaded some sort of file to my bulletin board that I had no knowledge of. This can and has happened to innocent unsuspecting people whose only crime was wanting to communicate with other computer users or download a public domain game.

Scenario: Joe Computeruser calls "The Games of Eternity BBS" one day hoping to get help on how to use his new spreadsheet package that he paid a large and legit sum of money for. He applies for an account and, as a result, his real name, age, address, and phone number (information that is required to gain access) are now stored in the BBS's user files. The sysop, Mr. Cool Joe Hacker, did something viciously malicious and has come under the scrutiny of the U.S. Government. His computer and all his files (and TV's, stereos, lamps, etc.) are confiscated, including the personal information of Joe Computeruser and countless other people who have accounts on the system. Joe Computeruser is now implicated in the investigation for collaborating in Mr. Cool Joe Hacker's exploits, along with the rest of the users on his BBS system, and is put under surveillance, even though he was calling for a most wholesome and legitimate reason. You don't think so, huh? Well, ignorance is bliss.

This government needs watching, not hackers. If hackers led the world, there wouldn't be half a million American troops in Saudi Arabia. Hackers don't send your sons and daughters to their deaths. The U.S. government does. While I cannot

totally say "do not fear the hacker," I can say "fear the government."

After all is said and done, there is a first. If a system exists that houses information, and you were not meant to be able to peruse that information then you do not have a constitutional right to be inside that system. But that's not to say that you won't go ahead and try to get into that system anyway. That's the choice you make, the rules of your game. There is such a thing as private property. That's one of the fundamental tenants our country is based upon. To use the argument that you have the right to be inside the computer systems of certain agencies gathering enormous amounts of information about you without your knowing, and to include in that argument that you have the right to be inside the computer systems of any private agency, company, etc. that houses information of any kind is not only entirely wrong, but stupid. But again, it all depends on the way the rules of your game are defined, the extent of your personal integrity, how screwed over you've ever been, and the way you look at life in general.

Since there will always be hackers, and there will always be those who think they have the right to be inside any system, the ultimate and unwavering responsibility lies on the owner of the system. If you don't make it secure enough, although you're not seeking for someone to break into it (who would be?), you've got to realize that not everyone out there gives a shit, and by golly if they want to hack into your system and they can, well then that's just what they're going to do. And that means that you overlooked something that you shouldn't have. That's life. That's the game.

If you enjoyed this issue, you may be interested in issues of the past. Move your eyes to the right for details.

## HURRY UP

Time is starting to run out. 1991 is sure to contain lots of unpleasant things, but one of the worst will be a price increase for 2600 subscribers. We're not raising the price out of malice or because of some distant dictator. This is not a sneaky attempt to raise money for war bonds or terrorist activity. Simply put, we're increasing our price because our costs have gone up: postage, printing, and so on. The same old story. By renewing your subscription now, you can still take advantage of the old prices. Because next issue just won't be the same.



### INDIVIDUAL SUBSCRIPTION

1 year/\$19  2 years/\$33  3 years/\$48

### CORPORATE SUBSCRIPTION

1 year/\$45  2 years/\$85  3 years/\$125

### OVERSEAS SUBSCRIPTION

1 year, individual/\$30  1 year, corporate/\$65

### LIFETIME SUBSCRIPTION

\$280 (you'll never have to deal with this again)

### BACK ISSUES (never out of date)

1984/\$25  1985/\$25  1986/\$25  1987/\$25

1988/\$25  1989/\$25

(OVERSEAS: ADD \$5 PER YEAR OF BACK ISSUES)

(individual back issues for 1989, 1989, 1990 are \$6.25 each)

TOTAL AMOUNT ENCLOSED: